

Veilig Online

Mijn Reis Naar Digitale Beveiliging

Veilig Online

Mijn Reis Naar Digitale Beveiliging

Marc Huyghebaert

Schrijver: Marc Huyghebaert
Coverontwerp: Brave New Books - Nederland
ISBN: 9789465013350
© Marc Huyghebaert
Uitgave versie : Eerste druk , versie Maart 2024
Gedrukt door: Brave New Books - Nederland

DISCLAIMER

Alle foto's in dit boek blijven eigendom van hun respectievelijke makers en mogen niet worden gereproduceerd, gekopieerd of gebruikt zonder hun uitdrukkelijke toestemming.

De genoemde merknamen zijn eigendom van hun respectieve bedrijven. We hebben geen banden met deze bedrijven, tenzij uitdrukkelijk vermeld.

Het is belangrijk om te begrijpen dat dit boek bedoeld is als een leidraad en niet als een exacte wetenschap. Hoewel het waardevolle inzichten en informatie biedt over cyberveiligheid, biedt het op zichzelf geen garantie of bescherming tegen mogelijke cyberbedreigingen.

Het is aan de lezer om deze informatie te gebruiken als onderdeel van een bredere strategie voor cyberveiligheid, die regelmatig moet worden geëvalueerd en aangepast om rekening te houden met veranderende bedreigingen en risico's.

We raden lezers dan ook aan om professioneel advies in te winnen en hun eigen onderzoek te doen voordat ze beveiligingsmaatregelen implementeren.

Niets uit deze publicatie mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt worden in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of op enige andere manier, zonder voorafgaande schriftelijke toestemming van de auteur of uitgever.

De auteur en de uitgever van dit boek hebben geprobeerd om de informatie in dit boek zo accuraat mogelijk weer te geven op het moment van publicatie. De auteur en de uitgever zijn echter niet verantwoordelijk voor eventuele fouten of weglatingen, of voor eventuele schade die voortvloeit uit het gebruik van de informatie in dit boek.

Voor vragen over de rechten voor publicatie van dit boek of voor meer informatie over de auteur, kunt u contact opnemen via info@ethisch-hacker.be.

DANKWOORD

Graag wil ik mijn dankbaarheid uitspreken aan iedereen die de tijd heeft genomen om mijn teksten na te lezen, tests uit te voeren en mij te inspireren, moed te geven, kracht te bieden en te steunen op momenten waarop ik het gevoel had dat ik niet verder kon. Jullie steun heeft mij geholpen om door te zetten en het beste uit mezelf te halen.

Het is niet altijd gemakkelijk om een project of doel te bereiken en ik ben me ervan bewust dat ik dit niet alleen had kunnen doen. De steun en feedback die ik heb ontvangen hebben mij geholpen om mijn werk te verbeteren en te groeien als persoon.

Ik realiseer me ook dat het niet vanzelfsprekend is dat mensen hun tijd en energie steken in de ondersteuning van anderen. Ik waardeer het daarom des te meer dat er mensen zijn die dat wel doen. Jullie hebben mijn leven verrijkt en ik zal jullie steun nooit vergeten.

Nogmaals, hartelijk dank voor jullie steun en aanmoediging. Ik zal deze ervaring koesteren en als motivatie gebruiken voor toekomstige uitdagingen en doelen die ik wil bereiken.

VOORWOORD

Het doel van dit verzamelboek is om u een waardevol instrument en handvat te bieden, waarmee u uw online veiligheid kunt waarborgen en beschermen.

Cybersecurity is een complexe uitdaging en er zijn veel factoren die afzonderlijk of gezamenlijk uw veiligheid in gevaar kunnen brengen. Dit verzamelboek biedt inzicht in de belangrijkste bedreigingen en risico's waarmee u online te maken kunt krijgen en geeft praktische adviezen en oplossingen om deze risico's te verminderen.

Om uw cybersecurity verder te verbeteren, bieden wij op maat gemaakte trainingen aan. Onze trainingen zijn gericht op het vergroten van uw bewustzijn van de gevaren van het internet en op het aanleren van effectieve technieken en 'best practices' om uzelf te beschermen. We begrijpen dat elke persoon en elk bedrijf anders is en daarom bieden we trainingen die speciaal zijn afgestemd op uw individuele behoeften en eisen.

Onze toewijding ligt bij het verbeteren van uw online veiligheid en het voorzien van de nodige tools en kennis om veilig te blijven in de digitale wereld. Wij begrijpen dat het belangrijk is om op de hoogte te blijven van de nieuwste technieken en bedreigingen, en daarom bieden wij voortdurend actuele informatie en trainingen aan om u te helpen. Onze missie is om u te ondersteunen bij het creëren van een veilige online omgeving voor uzelf, uw gezin en/of uw bedrijf.

Als men een schoendoos neemt, dan is de grootte ervan bekend. Bij Cybersecurity en hacking is er echter geen grootte of vast einde. Ieder moment van de dag komt er wel iets nieuws bij. Voor mij persoonlijk gaat het erom de computergebruiker bewust te maken van de gevaren van het internet.

Dagelijks horen we in het nieuws over mensen die in de val zijn getrapt. En nu komt iets wat velen niet graag zullen horen, maar meestal is het hun eigen schuld of hebben ze (onbewust) mee bijgedragen aan de oplichting of inbreuk. Onbewust, maar het had voorkomen kunnen worden.

Ik ga dus proberen om zoveel mogelijk technische en juridische zaken uit te leggen. In onze Cybersecurity Awareness Trainingen kunnen wij u effectief laten zien hoe Phishing werkt, hoe men uw pc, gsm, camera of microfoon kan overnemen, enzovoort. Hoe dit precies in zijn werk gaat, hoeft u niet in dit boek te verwachten. Dit is geen handleiding voor aspirant-hackers, laten we dat duidelijk stellen.

Iets leren en kunnen is één ding, het vertellen en tonen gaat nog wel, maar het op papier zetten is totaal iets anders. We gaan dus ons best doen.

Veel leesplezier!

BIO

Mijn naam is Marc Huyghebaert. Ik behaalde mijn eerste certificaat voor ethisch hacken in augustus 2021, gevolgd door mijn Bachelor in Security Management in december van datzelfde jaar.

Een essentieel aspect van Security Management is hacking en ik blijf mezelf voortdurend bijscholen door het volgen van cursussen. Mijn doel is om mensen van alle leeftijden bewust te maken van het belang van cybersecurity en in het bijzonder van hacking. Het internet kan namelijk een gevaarlijke plek zijn en het is belangrijk dat mensen zich bewust zijn van de mogelijke risico's en gevaren.

Als cybersecurity-professional wil ik mensen laten zien hoe criminelen hen kunnen aanvallen en vooral hoe ze zichzelf kunnen beschermen tegen deze bedreigingen. Door het vergroten van het bewustzijn en het delen van mijn kennis en expertise hoop ik bij te dragen aan een veiligere digitale wereld voor ons allemaal.

Inhoudstafel

1. Hoe het internet werkt.
2. Privacy, uw recht.
3. Oh nee. Uw wachtwoord werd gelekt of u bent gehackt.
4. Wat is OSiNT
5. QR-Code's
6. Wat zijn beacons
7. Beveiligscamera's
8. Bonus – Tips – Meer veiligheid – Allerlei info
9. Bluetooth and Mousejacking
10. Wat is een SIEM?
11. Windows Sandbox
12. Data Verbergen
13. Het belang van onze digitale voetafdruk
14. Metadata
15. USB-Datablockers
16. Op vakantie? Denk even na
17. A.i. en hacking
18. Achtergrondinformatie Wi-Fi Protected Setup of WPS
19. Het Dubbele Snijvlak van URL Shorteners:
20. WPS en de gevaren errond
21. URL Shorters en de mogelijke gevaren
22. De Travel Router
23. Captive portal en zijn Evil twin
24. Bitdefenter
25. Het verborgen gevaar
26. Wat is telefoon vervalsing (spoofing)
27. Wat is VoIP en is dat veilig?
28. Afsluiter
29. Links

Het internet

Het internet is een wereldwijd netwerk van computers dat informatie en gegevens met elkaar deelt. Het werkt op basis van een reeks protocollen en technologieën die ervoor zorgen dat computers over de hele wereld met elkaar kunnen communiceren.

Om te beginnen hebben we de basisbouwstenen van het internet: computers. Computers zijn apparaten die zijn uitgerust met speciale software en hardware om verbinding te maken met het internet. Elke computer die is verbonden met het internet, wordt een "host" genoemd.

Het internet maakt gebruik van een communicatieprotocol dat bekend staat als het Internet Protocol (IP). Elke computer die is verbonden met het internet heeft een uniek IP-adres, dat fungeert als een soort digitaal identificatienummer. Dit IP-adres maakt het mogelijk voor computers om elkaar te vinden en informatie uit te wisselen.

Wanneer een computer gegevens wil verzenden naar een andere computer op het internet, wordt de informatie opgedeeld in kleine pakketjes. Elk pakketje bevat de bron- en doel-IP-adressen, evenals een deel van de gegevens. Deze pakketjes worden via het internet naar hun bestemming gestuurd.

Om ervoor te zorgen dat de pakketjes de juiste bestemming bereiken, wordt gebruikgemaakt van routers. Routers zijn speciale computers die de pakketjes doorsturen naar andere routers totdat ze uiteindelijk hun bestemming bereiken. Routers gebruiken complexe algoritmen en tabellen om te bepalen waar de pakketjes naartoe moeten worden gestuurd om de meest efficiënte route te vinden.

Een ander belangrijk aspect van het internet is het Domain Name System (DNS). Aangezien IP-adressen niet erg gemakkelijk te onthouden zijn, wordt het DNS gebruikt om namen van websites om te zetten naar IP-adressen. Wanneer je bijvoorbeeld een website wilt bezoeken, typ je de domeinnaam in je webbrowser. De browser vraagt vervolgens het IP-adres van die domeinnaam op bij een DNS-server, waardoor de browser de juiste IP-adressen kan vinden en de website kan openen.

Om ervoor te zorgen dat gegevens veilig worden verzonden over het internet, wordt gebruikgemaakt van beveiligingsprotocollen zoals SSL (Secure Sockets Layer) of zijn opvolger TLS (Transport Layer Security). Deze protocollen versleutelen de gegevens tijdens de overdracht, waardoor het moeilijk wordt voor kwaadwillende om de gegevens te onderscheppen of te lezen.

Ten slotte, om inhoud op het internet te hosten en toegankelijk te maken, worden servers gebruikt. Servers zijn krachtige computers die speciale software draaien om webpagina's, bestanden en andere inhoud op te slaan en te leveren aan gebruikers die erom vragen.

Samengevat maakt het internet gebruik van een combinatie van computers, protocollen, routers, DNS en servers om informatie over de hele wereld te verzenden en toegankelijk te maken. Het is een complex systeem dat ons in staat stelt om te communiceren, informatie op te zoeken, te delen en te genieten van een breed scala aan online diensten en mogelijkheden.

Het begint allemaal met een IP-adres.

Wat is een IP-adres? Waarom is het nodig, maar ook potentieel gevaarlijk? Wat is een DNS-server? Wat is een domeinnaam? We zullen deze vragen beantwoorden hier proberen zo eenvoudig mogelijk te beantwoorden.

Een diepgaande blik op IP-adressen:

Het Ontstaan, Het Verschil tussen IPv4 en IPv6, en Interne en Externe IP-adressen

Introductie:

In de huidige digitale wereld is het begrijpen van IP-adressen essentieel. Of je nu een fervente internetgebruiker bent of een professional in de IT-sector, kennis van IP- adressen helpt je de fundamenten van het internet te begrijpen. In dit artikel zullen we een diepgaande blik werpen op IP-adressen, hun ontstaan, het verschil tussen IPv4 en IPv6, en het onderscheid tussen interne en externe IP-adressen.

Het Ontstaan van IP-adressen:

IP-adressen zijn ontstaan als een systeem om unieke identificatie toe te wijzen aan elk apparaat dat is verbonden met een computernetwerk. In de beginjaren van het internet, werd het Internet Protocol versie 4 (IPv4) geïntroduceerd. IPv4-adressen bestaan uit vier reeksen cijfers, gescheiden door punten. Elke reeks kan variëren van 0 tot 255, waardoor er ongeveer 4,3 miljard unieke IPv4-adressen beschikbaar zijn.

Vergelijk een IP-adres met uw huisnummer die een adres heeft, een identificatiemiddel voor elk apparaat dat verbonden is met internet. Wanneer je een apparaat met je router verbindt, via een kabel of wifi, krijgt dat apparaat automatisch een uniek IP-adres toegewezen binnen uw netwerk, door de router. Dit zijn de interne IP-adressen.

Daarnaast krijgt elke router die verbonden is met internet een extern IP-adres toegewezen, dit gebeurt door de internet provider.

Het Verschil tussen IPv4 en IPv6:

Met de exponentiële groei van internetgebruik en de toenemende behoefte aan meer unieke IP-adressen, kwam IPv4 op een punt waarop de beschikbare adressen bijna waren uitgeput. Dit leidde tot de ontwikkeling van het Internet Protocol versie 6 (IPv6). In tegenstelling tot IPv4, bestaat een IPv6-adres uit acht groepen van vier hexadecimale cijfers, gescheiden door dubbele punten. Dit resulteert in een enorme toename van het aantal beschikbare IP-adressen, met een totaal van ongeveer 340 undeciljoen ($3,4 \times 10^{38}$) adressen.

Interne IP-adressen:

Interne IP-adressen worden gebruikt binnen een lokaal netwerk (Local Area Network of LAN). Ze dienen om apparaten binnen het netwerk te identificeren en communicatie tussen deze apparaten mogelijk te maken. Bij een typisch thuisnetwerk worden interne IP-adressen toegewezen door de router via het Dynamic Host Configuration Protocol (DHCP). De meest voorkomende reeks interne IP-adressen is 192.168.0.0 tot 192.168.255.255, waarbij het derde en vierde octet variabel zijn.

Interne IP-adressen zijn bedoeld om te identificeren met welk specifiek apparaat uw router communiceert. In het voorbeeld xxx.xxx.x(xx).x(xx), houdt de notatie in dat de derde en vierde groep cijfers niet noodzakelijk uit drie cijfers hoeven te bestaan.

IP-adressen die beginnen met 192.xxx.x(xx).x(xx) zijn interne adressen binnen jouw LAN-netwerk, dus achter jouw router. Bijvoorbeeld, 192.168.0.1 is een intern IP-adres dat door je router wordt toegewezen. Het kan dus voorkomen dat je buurman in zijn LAN ook hetzelfde IP-adres toegewezen krijgt.

Het belangrijkste om te onthouden is dat een IP-adres dat begint met 192.xxx.x(xx).x(xx) een intern IP-adres is, specifiek voor jouw netwerk. Er kunnen en er mogen zelfs geen 2 toestellen met hetzelfde ip adres verbonden zijn met uw router, want dan weet deze niet meer met wie de router een het communiceren is.

“Router” is het bakje aan de muur die u van uw internetprovider kreeg.

“Lan” is uw intern thuis netwerk, dit kan volledig uit een wifi netwerk bestaan, of een mix met toestellen verbonden met een kabel.

Externe IP-adressen:

Externe IP-adressen worden gebruikt voor communicatie tussen het lokale netwerk en externe netwerken, zoals het internet. Een externe IP-adres wordt toegewezen aan de router of het modem dat het lokale netwerk met het internet verbindt. Dit adres fungeert als een unieke identificatie voor het netwerk op het internet. Internetproviders kunnen dynamische of statische externe IP-adressen toewijzen aan gebruikers, afhankelijk van het type internetabonnement. Het externe IP adres is dus verbonden met uw fysieke locatie, uw huis of kantoor in de meeste gevallen.

In het kort samengevat

IP-adressen vormen de ruggengraat van het internet en zijn cruciaal voor het mogelijk maken van communicatie tussen apparaten en netwerken. Het ontstaan van IP-adressen begon met IPv4, dat vier reeksen cijfers gebruikte en ongeveer 4,3 miljard unieke adressen bood. Met de groeiende behoefte aan meer adressen en de introductie van IPv6 met zijn acht reeksen hexadecimale cijfers, werd het aantal beschikbare adressen drastisch vergroot naar een duizelingwekkend aantal.

Interne IP-adressen worden gebruikt binnen een lokaal netwerk om apparaten te identificeren en de communicatie tussen hen mogelijk te maken. Deze adressen worden toegewezen door de router. Interne IP-adressen zijn alleen geldig binnen het lokale netwerk en worden niet rechtstreeks op het internet verbonden.

Aan de andere kant worden externe IP-adressen toegewezen aan de router of het modem dat het lokale netwerk verbindt met het internet. Dit externe IP-adres fungeert als een unieke identificatie voor het netwerk op het internet. Internetproviders kunnen dynamische externe IP-adressen toewijzen die periodiek kunnen veranderen, of statische externe IP-adressen die permanent aan het netwerk zijn gekoppeld.

Externe IP-adressen zijn essentieel voor de communicatie tussen het lokale netwerk en externe netwerken, waardoor apparaten toegang krijgen tot internetdiensten en informatie kunnen uitwisselen met andere netwerken over de hele wereld.

IP-adressen zijn de essentiële bouwstenen van het internet en spelen een cruciale rol bij het mogelijk maken van communicatie tussen apparaten en netwerken. Het begrijpen van de verschillen tussen IPv4 en IPv6, evenals het onderscheid tussen interne en externe IP-adressen, stelt gebruikers in staat om optimaal gebruik te maken van het internet en de voordelen ervan ten volle te benutten.

Hoe kan je weten wat uw externe IP adres is en wat het gebruikte toestel zijn interne IP is onder Windows?

- Ga naar de start knop, type onderaan CMD
- Eenmaal in terminal mode type dan ipconfig

dan krijg je zoiets te zien Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::8993:b1f9:1d99:1d6c%19  
IPv4 Address. . . . . : 192.168.1.238 (dit is dus het intern ip  
adres van mijn PC toegekend door mijn router)  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.1.1 (dit is het "vast" ip adres  
van de router, de eerste in de rij dus)  
xxx.xxx.255.255 zou dan de laatste zijn
```

Zover de Interne IP adressen binnen uw lokaal netwerk.

Zoals eerder gezegd krijgt uw Router (uw woning) ook een IP adres toegewezen van uw provider (wie dat ook is) dat is uw extern of ook wel publiek IP adres genaamd. Zo komt u naar de buitenwereld.

Nu zijn eigenlijk hier een paar gevaren aan verbonden, namelijk uw publiek IP adres is aan U verbonden, net zoals de nummerplaat van uw auto dus.

Wil je weten wat uw publiek IP adres is en welke informatie u zo vrij onthuld?

<https://video.ethisch-hacker.be/mijnpubliekipadres.php>

We hebben dit gemaakt om u te tonen welke informatie u al onthuld, er is nog veel meer maar dit berspreken we verder in het boek (OSiNT).

Hoe denk je dat bepaalde bedrijven waarvan u de website bezocht u kort nadien een reclame folder toesturen? Deze informatie is voor veel bedrijven (Facebook/Google/....) veel geld waard. Maar zoals reeds gezegd dat is informatie verder uitgelegd in het OSiNT onderdeel van dit verzamelboek.

Belangrijk te weten is dat uw publiek IP adres niet zo onschuldig is en u dat eigenlijk beter maskeert, en/of verbergt. dat kan op diverse manieren meer info hierover verder in dit boek.

Wat is een domeinnaam?

Na het begrijpen van IP-adressen en het feit dat alle apparaten die verbonden zijn met internet een IP-adres hebben, komen we bij het volgende probleem: het zou onpraktisch zijn om bij het surfen naar een website telkens het IP-adres van de server in te voeren.

Stel je voor dat je elke keer 142.251.39.99 moet typen om Google.be te bezoeken. Dat zou erg onhandig zijn.

Om dit probleem op te lossen, zijn domeinnamen bedacht. Domeinnamen, ook wel bekend als URL's of links, fungeren als mensvriendelijke namen voor websites. Ze zijn makkelijk te onthouden en typen, waardoor het navigeren op het internet veel eenvoudiger wordt.

Het proces van het vertalen van een domeinnaam naar het bijbehorende IP-adres wordt uitgevoerd door een DNS-server (Domain Name Server). Een DNS-server fungeert als een soort vertaler die de domeinnaam, zoals Google.be, omzet naar het IP-adres van de server waar de website zich bevindt. In ons voorbeeld zou de DNS-server Google.be omzetten naar het IP-adres 142.251.39.99, waar de server van de Google-website zich bevindt.

Het hele proces van het omzetten van domeinnamen naar IP-adressen gebeurt automatisch en is iets waar de meeste internetgebruikers zich geen zorgen over hoeven te maken. Het is echter belangrijk op te merken dat op dit niveau een hacker kan proberen in te grijpen door de DNS-route te wijzigen. Dit kan leiden tot omleiding van gebruikers naar valse websites of andere kwaadaardige activiteiten. Gelukkig zijn er beveiligingsmaatregelen en protocollen om dit risico te beperken.

Domeinnamen zijn dus mensvriendelijke namen voor websites die het gemakkelijk maken om te navigeren op het internet. DNS-servers zorgen voor het vertalen van deze domeinnamen naar de bijbehorende IP-adressen, waardoor de communicatie tussen gebruikers en servers mogelijk wordt gemaakt. Het begrijpen van dit proces helpt ons de werking van het internet beter te begrijpen en bewust te zijn van mogelijke beveiligingsrisico's.

Belangrijk om te onthouden is dat er principieel twee soorten IP-adressen zijn: interne IP-adressen binnen uw lokale netwerk en uw publieke IP-adres. Deze twee adressen hebben verschillende functies en implicaties.

Uw interne IP-adres wordt gebruikt binnen uw lokale netwerk om apparaten te identificeren en communicatie mogelijk te maken. Dit adres is alleen geldig binnen uw privé-netwerk en wordt niet rechtstreeks blootgesteld aan het internet. Het wordt toegewezen door uw router en is van vitaal belang voor het routeren van gegevens tussen apparaten in uw netwerk.

Aan de andere kant hebben we het publieke IP-adres, dat is het adres waarmee uw netwerk naar buiten toe wordt geïdentificeerd op het internet. Dit adres wordt toegewezen door uw internetprovider en wordt gebruikt om communicatie met externe netwerken mogelijk te maken. Wanneer u verbinding maakt met een website of een online service, wordt uw publieke IP-adres gebruikt om gegevens heen en weer te sturen.

Het is belangrijk om te weten dat uw publieke IP-adres niet zonder gevaar is. Het onthult bepaalde informatie over u, zoals uw algemene locatie en uw internetprovider. Hoewel het niet uw exacte fysieke locatie onthult, kan het nog steeds gevoelige informatie bevatten die mogelijk kan worden misbruikt. Daarom is het belangrijk om veiligheidsmaatregelen te treffen, zoals het gebruik van firewalls en VPN's, om uw privacy en online beveiliging te beschermen.

Een DNS-server speelt een cruciale rol bij het verbinden van domeinnamen met bijbehorende IP-adressen. Wanneer u een domeinnaam in uw webbrowser invoert, raadpleegt uw apparaat een DNS-server om het bijbehorende IP-adres van die domeinnaam te verkrijgen. Dit proces maakt het voor u als gebruiker veel gemakkelijker om websites te bezoeken, omdat u alleen een herkenbare naam hoeft in te voeren in plaats van een reeks cijfers.

Kortom, het begrijpen van de verschillende soorten IP-adressen, met name interne en publieke IP-adressen, helpt u de werking van uw netwerk en de implicaties ervan beter te begrijpen. Het is ook belangrijk om bewust te zijn van de privacy risico's die gepaard gaan met uw publieke IP-adres en om passende maatregelen te nemen om uw online veiligheid te waarborgen. De rol van DNS-servers bij het koppelen van domeinnamen aan IP-adressen maakt het gemakkelijker voor gebruikers om het internet te verkennen en websites te bezoeken.

Wanneer een gebruiker een link invoert in een webbrowser en vervolgens op enter drukt, gebeurt er achter de schermen een aantal stappen om de gewenste webpagina weer te geven. Hier is een overzicht van wat er gebeurt:

DNS-resolutie: De webbrowser begint met het verwerken van de ingevoerde link, die meestal een domeinnaam bevat (bijv. www.example.com). De browser moet het IP-adres van de webserver vinden waarop de gevraagde webpagina zich bevindt. Om dit te doen, stuurt de browser een verzoek naar een DNS-server om het IP-adres van de domeinnaam op te zoeken. De DNS-server vertaalt de domeinnaam naar het bijbehorende IP-adres.

Het opzetten van een TCP-verbinding: Met het IP-adres in handen, kan de browser nu een verbinding maken met de webserver waarop de gevraagde webpagina zich bevindt. Dit gebeurt via het Transmission Control Protocol (TCP). TCP zorgt ervoor dat de gegevens betrouwbaar kunnen worden overgedragen tussen de browser en de server.

Het verzenden van een HTTP-verzoek: Zodra de TCP-verbinding tot stand is gebracht, stuurt de browser een HTTP-verzoek naar de webserver. Het HTTP-verzoek bevat informatie zoals het type verzoek (bijvoorbeeld GET, POST, etc.), de gewenste webpagina en eventuele extra parameters.

Verwerking van het verzoek door de webserver: De webserver ontvangt het HTTP-verzoek van de browser en begint het te verwerken. Het zoekt de gevraagde webpagina op de server en voert eventuele vereiste taken uit, zoals het ophalen van gegevens uit een database.

Het genereren van een HTTP-respons: Nadat de webserver de gevraagde webpagina heeft gevonden en alle benodigde taken heeft voltooid, genereert het een HTTP-respons. Deze respons bevat de gevraagde webpagina en informatie zoals de statuscode (bijvoorbeeld 200 voor succesvolle respons), inhoudstype (bijvoorbeeld HTML, afbeeldingen, JavaScript, enz.) en andere optionele headers.

Het verzenden van de HTTP-respons: De webserver stuurt de gegenereerde HTTP-respons terug naar de browser via de eerder geopende TCP-verbinding. De respons wordt opgedeeld in pakketjes die via het internet naar de browser worden gestuurd.

Het weergeven van de webpagina: Zodra de browser de HTTP-respons heeft ontvangen, begint hij met het verwerken ervan. Hij controleert de statuscode om te bepalen of het verzoek succesvol was en interpreteert de ontvangen inhoud (bijv. HTML) om de webpagina correct weer te geven. Dit omvat het renderen van tekst, afbeeldingen, opmaak en eventuele interactieve elementen op de webpagina.

Aanvullende verzoeken: Als de ontvangen webpagina verwijzingen bevat naar andere bronnen, zoals afbeeldingen, JavaScript-bestanden of CSS-stijlbladen, zal de browser aanvullende HTTP-verzoeken verzenden om die bronnen op te halen. Dit stelt de browser in staat om de webpagina volledig te laden en weer te geven.

Deze aanvullende verzoeken worden gedaan om de bronnen te verkrijgen die nodig zijn voor de volledige weergave en functionaliteit van de webpagina. De browser identificeert de verwijzingen naar externe bronnen, zoals afbeeldingen, door de HTML- code te analyseren.

Voor elke externe bron wordt een nieuw HTTP-verzoek gemaakt en verzonden naar de bijbehorende server. Dit verzoek bevat informatie zoals het gewenste bestand (afbeelding, JavaScript, CSS) en de locatie ervan. Zodra de server het verzoek ontvangt, zoekt het de gevraagde bron op en stuurt het een HTTP-respons terug naar de browser.

Deze respons bevat de gevraagde bron, zoals een afbeelding of een JavaScript-bestand. Na ontvangst van de bron begint de browser met het verwerken ervan. Afbeeldingen worden geladen en weergegeven op de juiste positie op de webpagina. JavaScript- bestanden worden uitgevoerd, waardoor interactieve functionaliteiten worden toegevoegd aan de webpagina. CSS-stijlbladen worden toegepast om de visuele stijl van de webpagina aan te passen.

Op deze manier kunnen gebruikers, wanneer ze een link invoeren en de webpagina te zien krijgen, genieten van een rijke en interactieve online ervaring waarbij alle benodigde bronnen correct worden geladen en weergegeven.

Laden van externe bronnen: Als de webpagina verwijzingen bevat naar externe bronnen, zoals afbeeldingen, stijlbladen of JavaScript-bestanden, zal de browser aanvullende HTTP-verzoeken verzenden om die bronnen op te halen. Deze bronnen worden meestal gehost op verschillende servers. De browser maakt nieuwe TCP-verbindingen met de betreffende servers en vraagt de specifieke bronnen op. Zodra de bronnen zijn gedownload, worden ze door de browser geïntegreerd in de weergave van de webpagina.

Zodra alle externe bronnen zijn geladen en verwerkt, is de webpagina volledig geladen en klaar om aan de gebruiker te worden getoond. Alle elementen, inclusief de inhoud, afbeeldingen, stijlen en functionaliteiten, worden samengevoegd en weergegeven volgens de specificaties van de HTML en CSS.

Uitvoering van JavaScript-code: Als de webpagina JavaScript-code bevat, zal de browser deze code uitvoeren. JavaScript kan worden gebruikt om interactieve elementen en dynamische functionaliteiten op de webpagina toe te voegen. De browser interpreteert de JavaScript-instructies en voert ze uit, waardoor de webpagina dynamisch kan reageren op gebruikersinteracties of andere gebeurtenissen.

Weergave van de volledige webpagina: Na het laden van alle vereiste bronnen en het uitvoeren van eventuele JavaScript-code, is de browser klaar om de volledige webpagina weer te geven aan de gebruiker. De gebruiker ziet nu de inhoud van de webpagina, inclusief tekst, afbeeldingen, opmaak, interactieve elementen en eventuele functionaliteiten die zijn geïmplementeerd met behulp van JavaScript.

Het hele proces van het invoeren van een link en het weergeven van de webpagina gebeurt binnen enkele seconden. Het omvat het opzetten van een verbinding met de webserver, het verzenden van een HTTP-verzoek, het ontvangen en verwerken van de HTTP-respons, het laden van externe bronnen en het uitvoeren van JavaScript-code om een volledige en interactieve web-ervaring te bieden aan de gebruiker.

HTTP vs HTTPS

HTTP en HTTPS zijn beide protocollen die worden gebruikt voor de communicatie tussen een webbrowser en een webserver. Het belangrijkste verschil tussen de twee is de beveiliging van de gegevensoverdracht.

HTTP staat voor Hypertext Transfer Protocol en is het standaardprotocol dat wordt gebruikt voor het verzenden en ontvangen van gegevens over het internet. Met HTTP worden de gegevens on-versleuteld verzonden, wat betekent dat ze in leesbare vorm worden verstuurd. Dit maakt het gemakkelijk voor aanvallers om de gegevens te onderscheppen en te lezen. Daarom wordt HTTP als een onveilig protocol beschouwd.

HTTPS staat voor Hypertext Transfer Protocol Secure en is een beveiligde versie van HTTP. HTTPS maakt gebruik van een extra beveiliging laag genaamd SSL (Secure Sockets Layer) of zijn opvolger TLS (Transport Layer Security). Deze beveiliging laag versleutelt de gegevens tijdens de overdracht, waardoor het moeilijk wordt voor kwaadwillende om de gegevens te onderscheppen of te lezen. Hierdoor is HTTPS veel veiliger dan HTTP.

Het belangrijkste beveiligingsvoordeel van HTTPS is dat het de vertrouwelijkheid en integriteit van gegevens beschermt. Vertrouwelijkheid wordt bereikt door het versleutelen van de gegevens, zodat alleen de beoogde ontvanger ze kan lezen.

Integriteit betekent dat de gegevens tijdens de overdracht niet kunnen worden gewijzigd of gemanipuleerd door derden. HTTPS zorgt er ook voor dat de gebruiker daadwerkelijk communiceert met de juiste website, omdat het gebruikmaakt van digitale certificaten die de authenticiteit van de website verifiëren.

Om HTTPS te gebruiken, moet een website een SSL/TLS-certificaat hebben dat wordt uitgegeven door een vertrouwde certificaatautoriteit. Dit certificaat bevestigt dat de website legitiem is en dat de gegevens veilig kunnen worden verzonden.

Kortom, HTTPS is veiliger dan HTTP omdat het de gegevens versleutelt en de integriteit van de gegevensoverdracht waarborgt. Het gebruik van HTTPS is vooral belangrijk bij het verzenden van gevoelige informatie, zoals inloggegevens, creditcardgegevens en persoonlijke gegevens, omdat het de risico's van gegevensinbreuken en afluisteren minimaliseert.

Privacy uw recht

Het fundamentele recht op privacy is een belangrijk aspect van de mensenrechten. Het is het recht van individuen om zelf te bepalen welke informatie over hen wordt verzameld, hoe deze informatie wordt gebruikt en wie er toegang heeft tot deze informatie.

Het recht op privacy is vastgelegd in verschillende internationale verdragen en verklaringen, waaronder de Universele Verklaring van de Rechten van de Mens en het Europees Verdrag voor de Rechten van de Mens. Het is ook opgenomen in nationale grondwetten en wetgevingen.

Het recht op privacy omvat verschillende aspecten, zoals het recht op persoonlijke levenssfeer, het recht op vertrouwelijkheid van communicatie, het recht op bescherming van persoonsgegevens en het recht op geheimhouding van persoonlijke informatie.

Het recht op persoonlijke levenssfeer omvat het recht van individuen om in hun eigen woning te wonen zonder inbreuk te maken op hun privacy. Dit omvat ook het recht om te bepalen wie er toegang heeft tot hun woning en welke informatie er over hen wordt verzameld en opgeslagen.

Het recht op vertrouwelijkheid van communicatie omvat het recht van individuen om vrijelijk te communiceren zonder dat hun communicatie wordt afgeluisterd of afgeluisterd door derden. Dit omvat ook het recht om te bepalen wie er toegang heeft tot hun communicatie en om te bepalen welke informatie er wordt gedeeld.

Het recht op bescherming van persoonsgegevens omvat het recht van individuen om te bepalen welke informatie er over hen wordt verzameld en hoe deze informatie wordt gebruikt. Dit omvat ook het recht om te weten welke informatie er over hen wordt verzameld en om toestemming te geven voor het gebruik van hun informatie.

Het recht op geheimhouding van persoonlijke informatie omvat het recht van individuen om te voorkomen dat hun persoonlijke informatie wordt verspreid zonder hun toestemming. Dit omvat ook het recht om te bepalen wie er toegang heeft tot hun persoonlijke informatie en hoe deze informatie wordt gebruikt.

Het recht op privacy is van essentieel belang voor de bescherming van de individuele vrijheid en waardigheid. Het is belangrijk dat overheden, bedrijven en andere instellingen deze rechten respecteren en beschermen. Dit omvat het waarborgen van de veiligheid van persoonsgegevens, het beperken van de verzameling van persoonlijke informatie en het respecteren van het recht op vertrouwelijkheid van communicatie.

In deze moderne tijd waarin technologie ons leven beheerst, is het belangrijker dan ooit om het recht op privacy te beschermen. Er moet worden gestreefd naar een evenwicht tussen de bescherming van de privacy van individuen en de behoefte aan informatie van overheden en bedrijven. Door deze rechten te beschermen, kunnen we een veiligere en meer rechtvaardige samenleving creëren voor ons allemaal.

Het begrip Privacy

Privacy is een breed en complex begrip dat wordt gebruikt om verschillende aspecten van ons persoonlijke leven te beschrijven. Het verwijst naar het recht van individuen om hun persoonlijke informatie, gedachten en handelingen te beschermen tegen ongewenste of ongepaste inmenging van anderen, waaronder overheden, bedrijven en individuen. Privacy is een fundamenteel mensenrecht dat is vastgelegd in verschillende internationale en nationale wetten en verdragen, waaronder de Universele Verklaring van de Rechten van de Mens en het Europees Verdrag voor de Rechten van de Mens. Het is ook een belangrijk onderdeel van de moderne democratie en een essentieel onderdeel van de menselijke waardigheid en vrijheid.

Het begrip privacy omvat verschillende aspecten, waaronder:

- Fysieke privacy: dit verwijst naar het recht van individuen om vrij te zijn van ongewenste fysieke inmenging, zoals het betreden van hun woning zonder toestemming.
- Communicatie privacy: dit verwijst naar het recht van individuen om vrijelijk te communiceren zonder dat hun communicatie wordt afgeluisterd of gemonitord.
- Informatie privacy: dit verwijst naar het recht van individuen om te bepalen welke persoonlijke informatie er over hen wordt verzameld, hoe deze informatie wordt gebruikt en met wie deze informatie wordt gedeeld.
- Beslissing privacy: dit verwijst naar het recht van individuen om zelf te beslissen over persoonlijke kwesties, zoals hun lichaam, seksualiteit en reproductieve keuzes.

Privacy wordt vaak bedreigd door de opkomst van nieuwe technologieën, zoals sociale media, datamining en kunstmatige intelligentie. Deze technologieën maken het mogelijk om grote hoeveelheden persoonlijke informatie te verzamelen en te analyseren, wat de privacy van individuen kan schenden.

Om deze bedreigingen tegen te gaan, hebben overheden en organisaties de verantwoordelijkheid om de privacy van individuen te beschermen. Dit kan worden bereikt door middel van wetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG) in de Europese Unie, die bepaalt hoe persoonlijke informatie moet worden verzameld en verwerkt.

Individen hebben ook een rol te spelen in het beschermen van hun eigen privacy. Dit kan worden bereikt door middel van het bewust zijn van de risico's en gevaren van het delen van persoonlijke informatie online, het gebruik van privacy-instellingen op sociale media en het beperken van de hoeveelheid informatie die wordt gedeeld.

In een tijd waarin onze persoonlijke informatie gemakkelijk toegankelijk is voor anderen, is het belangrijk om onze privacy te beschermen. Het is een fundamenteel mensenrecht dat moet worden gerespecteerd en beschermd, en het is de verantwoordelijkheid van ons allemaal om ervoor te zorgen dat onze privacy wordt gerespecteerd en gewaarborgd.

Privacy en het internet

In de moderne wereld spelen privacy en het internet een belangrijke rol. Het internet heeft ons leven op vele manieren verbeterd en vergemakkelijkt, maar heeft ook geleid tot nieuwe uitdagingen op het gebied van privacy. In dit hoofdstuk zullen we kijken naar hoe privacy en het internet met elkaar verbonden zijn en welke maatregelen genomen kunnen worden om onze privacy op het internet te beschermen.

Een van de grootste uitdagingen van privacy op het internet is de enorme hoeveelheid persoonlijke informatie die we online delen. Social media platforms, e-commerce websites en andere online diensten verzamelen en bewaren enorme hoeveelheden persoonlijke informatie van gebruikers, zoals hun naam, adres, telefoonnummer, e-mailadres en geboortedatum. Deze informatie kan worden gebruikt om gerichte advertenties te tonen, maar kan ook worden misbruikt door hackers en andere kwaadwillende.

Een ander belangrijk probleem is het gebrek aan transparantie over hoe bedrijven omgaan met de persoonlijke informatie die ze verzamelen. Veel websites hebben vaak ondoorzichtige gebruiksvoorwaarden en privacy beleid, waardoor het voor gebruikers moeilijk is om te begrijpen wat er met hun gegevens gebeurt. Dit kan leiden tot een gebrek aan vertrouwen en onzekerheid over de bescherming van persoonlijke informatie.

Om deze uitdagingen het hoofd te bieden, zijn er verschillende maatregelen die we kunnen nemen om onze privacy op het internet te beschermen. Hieronder bespreken we er een paar:

- Gebruik sterke wachtwoorden: Een van de beste manieren om uw online privacy te beschermen, is door het gebruik van sterke en unieke wachtwoorden. Vermijd het gebruik van wachtwoorden die gemakkelijk te raden zijn, zoals '123456' of 'password'. Gebruik in plaats daarvan langere en complexere wachtwoorden, met een mix van letters, cijfers en symbolen.
- Beperk de hoeveelheid persoonlijke informatie die u online deelt: Probeer zoveel mogelijk te beperken welke persoonlijke informatie u online deelt. Dit betekent dat u bijvoorbeeld geen gevoelige informatie zoals uw rijksregister nummer of creditcardgegevens online plaatst.
- Zorg voor sterke privacy-instellingen: Veel sociale media en andere online platforms hebben privacy-instellingen waarmee u kunt bepalen wie uw persoonlijke informatie kan zien. Zorg ervoor dat u deze instellingen begrijpt en gebruik maakt van deze opties om uw persoonlijke informatie te beschermen.
- Gebruik een VPN: Een VPN (Virtual Private Network) is een service die uw internetverkeer versleutelt en omleidt via een beveiligde server. Hierdoor wordt het moeilijker voor hackers om toegang te krijgen tot uw persoonlijke informatie.
- Houd uw software up-to-date: Zorg ervoor dat u uw software, zoals uw besturingssysteem en antivirussoftware, regelmatig bijwerkt om ervoor te zorgen dat uw computer beschermd blijft tegen de nieuwste bedreigingen.

In conclusie, privacy en het internet zijn onlosmakelijk met elkaar verbonden. Hoewel het internet ons leven op vele manieren heeft verbeterd, is het ook belangrijk om de mogelijke risico's op het gebied van privacy te begrijpen en maatregelen te nemen om onze persoonlijke informatie te beschermen. Door het gebruik van sterke wachtwoorden, het beperken van de hoeveelheid persoonlijke informatie die we online delen, het instellen van sterke privacy-instellingen, het gebruik van een VPN en het bijwerken van onze software, kunnen we ons online veiliger voelen en onze persoonlijke informatie beschermen.

Daarnaast is het ook belangrijk dat bedrijven meer transparantie bieden over hoe ze omgaan met de persoonlijke informatie van gebruikers en dat er meer regulering en toezicht komt om de privacy op het internet te beschermen. Dit kan bijvoorbeeld worden bereikt door middel van wetgeving zoals de AVG (Algemene verordening gegevensbescherming), die bedrijven verplicht om duidelijke privacy beleid te hebben en toestemming te vragen voor het verzamelen van persoonlijke informatie.

Uiteindelijk is het aan ons als individuen om ons bewust te zijn van de risico's op het gebied van privacy en om maatregelen te nemen om onze persoonlijke informatie te beschermen. Door ons hiervan bewust te zijn en proactief te handelen, kunnen we genieten van de voordelen van het internet zonder onze privacy op te offeren.

Wat is nu 'De Algemene verordening gegevensbescherming (AVG)'?

De Algemene verordening gegevensbescherming (AVG) is een wetgeving van de Europese Unie die op 25 mei 2018 in werking trad. Het is ontworpen om de privacy rechten van individuen binnen de EU te beschermen en om de manier waarop bedrijven en organisaties omgaan met persoonlijke informatie te standaardiseren.

De AVG is van toepassing op alle bedrijven en organisaties, ongeacht hun locatie, die persoonlijke informatie van personen binnen de EU verwerken. Het heeft tot doel de privacy van burgers te beschermen door bedrijven te verplichten hun privacy praktijken te herzien, hun beleid en procedures bij te werken en transparantie te bieden over hoe zij omgaan met persoonlijke gegevens.

Een van de belangrijkste onderdelen van de AVG is de eis dat bedrijven en organisaties toestemming moeten krijgen van personen voordat ze hun persoonlijke gegevens verzamelen, gebruiken of delen. Dit betekent dat bedrijven en organisaties niet langer persoonlijke gegevens mogen verzamelen zonder de uitdrukkelijke toestemming van de persoon van wie de gegevens worden verzameld. Bovendien moet de toestemming duidelijk en begrijpelijk zijn, en kan deze te allen tijde worden ingetrokken.

Een ander belangrijk aspect van de AVG is het recht op toegang tot persoonlijke informatie. Personen hebben het recht om te weten welke informatie bedrijven en organisaties over hen hebben verzameld en waarvoor deze informatie wordt gebruikt. Als een persoon fouten of onjuistheden in hun persoonlijke gegevens ontdekt, hebben ze het recht om deze te laten corrigeren of verwijderen.

Bedrijven en organisaties zijn ook verplicht om de privacy van persoonlijke gegevens te waarborgen. Dit betekent dat ze de nodige maatregelen moeten nemen om persoonlijke gegevens te beschermen tegen ongeoorloofde toegang, vernietiging, wijziging of openbaarmaking. Bedrijven en organisaties moeten ook proactief risico's beoordelen en mitigeren en eventuele inbreuken op de beveiliging van gegevens melden aan de relevante autoriteiten en de betrokken personen.

Als bedrijven of organisaties zich niet aan de AVG houden, kunnen ze hoge boetes krijgen. De boetes kunnen oplopen tot 4% van de wereldwijde jaaromzet of €20 miljoen, afhankelijk van welk bedrag hoger is.

De invoering van de AVG heeft geleid tot een verhoogde aandacht voor gegevens-bescherming en privacy. Bedrijven en organisaties moeten nu hun privacy beleid en procedures regelmatig herzien en bijwerken om ervoor te zorgen dat ze voldoen aan de vereisten van de AVG. Ze moeten ook transparant zijn over hoe ze omgaan met persoonlijke gegevens en toestemming verkrijgen voordat ze deze gegevens verzamelen, gebruiken of delen.

De Algemene verordening gegevensbescherming is een belangrijke wetgeving die bedrijven en organisaties dwingt om hun privacy praktijken te herzien en te verbeteren. Het heeft tot doel de privacy rechten van burgers binnen de EU te beschermen en de controle over hun persoonlijke gegevens te vergroten. Het heeft ook geleid tot een verhoogde aandacht voor gegevensbescherming en privacy in het bedrijfsleven en bij organisaties.

De invoering van de AVG heeft ook geleid tot veranderingen in de manier waarop bedrijven en organisaties omgaan met persoonlijke gegevens. Ze moeten nu rekening houden met de privacy van persoonlijke gegevens en proactief stappen ondernemen om de beveiliging van gegevens te waarborgen. Het niet naleven van de AVG kan ernstige gevolgen hebben voor bedrijven en organisaties, inclusief hoge boetes en reputatieschade.

De AVG heeft ook gevolgen voor individuen. Het geeft hen meer controle over hun persoonlijke gegevens en stelt hen in staat om hun privacy rechten uit te oefenen. Personen hebben het recht om te weten welke informatie bedrijven en organisaties over hen hebben verzameld en waarvoor deze informatie wordt gebruikt. Ze hebben ook het recht om deze informatie te laten corrigeren of verwijderen als ze onjuist of ongepast is.

Kortom, de Algemene verordening gegevensbescherming is een belangrijke stap in de bescherming van privacy en persoonlijke gegevens. Het heeft geleid tot veranderingen in de manier waarop bedrijven en organisaties omgaan met persoonlijke gegevens en heeft individuen meer controle gegeven over hun persoonlijke gegevens. Het is belangrijk dat bedrijven en organisaties de AVG naleven en transparant zijn over hoe ze omgaan met persoonlijke gegevens om ervoor te zorgen dat de privacy van burgers wordt beschermd en gerespecteerd.

AVG of GDPR

Er is geen verschil tussen AVG en GDPR, het zijn dezelfde wetgevingen. De AVG (Algemene Verordening Gegevensbescherming) is de Nederlandse term voor de GDPR (General Data Protection Regulation).

Cookies en de wetgeving

Cookies zijn kleine tekstbestanden die worden opgeslagen op de computer of het apparaat van een gebruiker wanneer deze een website bezoekt. Ze worden gebruikt om informatie over het surfgedrag van een gebruiker te verzamelen, zoals bezochte pagina's, tijdstippen van bezoeken en zoektermen. Hoewel cookies nuttig kunnen zijn voor website-eigenaren en marketeers, is het belangrijk om op te merken dat het verzamelen van persoonlijke gegevens zonder toestemming van de gebruiker een schending kan zijn van de privacy van de gebruiker.

Daarom is er in de EU de Privacy Richtlijn en de Algemene verordening gegevens-bescherming (AVG/GDPR) ingevoerd om de privacy van gebruikers te beschermen en hun controle over hun persoonlijke gegevens te vergroten. Deze wetgeving verplicht websites en apps om duidelijke en transparante informatie te verstrekken over het gebruik van cookies en om toestemming te vragen aan gebruikers voor het plaatsen van cookies.

In de EU is het verplicht om gebruikers toestemming te vragen voordat er cookies op hun apparaat worden geplaatst. Dit betekent dat wanneer een gebruiker een website bezoekt, deze website de gebruiker moet informeren over het soort cookies dat de website gebruikt en waarvoor deze worden gebruikt. Dit moet in duidelijke en begrijpelijke taal worden gedaan, zodat de gebruiker een weloverwogen keuze kan maken over het accepteren of weigeren van cookies.

Als de gebruiker geen toestemming geeft voor het plaatsen van cookies, mogen de cookies niet op het apparaat van de gebruiker worden geplaatst, tenzij deze strikt noodzakelijk zijn voor het functioneren van de website. Dit betekent dat alleen cookies die essentieel zijn voor de werking van de website, zoals sessiecookies voor het inloggen, zonder toestemming kunnen worden geplaatst.

Bovendien moeten website-eigenaren en -beheerders de cookies duidelijk categoriseren en hun gebruikers informeren over de specifieke categorieën cookies die op hun website worden gebruikt. Dit kan bijvoorbeeld omvatten:

- Strikt noodzakelijke cookies: Deze zijn nodig om de website goed te laten functioneren en worden niet gebruikt om persoonlijke gegevens te verzamelen.
- Functionele cookies: Deze worden gebruikt om de gebruikerservaring te verbeteren en om bepaalde functies op de website mogelijk te maken.
- Prestatiecookies: Deze worden gebruikt om gegevens te verzamelen over hoe de gebruiker de website gebruikt en om de prestaties van de website te verbeteren.
- Targetingcookies: Deze worden gebruikt om advertenties af te stemmen op de interesses van de gebruiker.

Het is belangrijk voor website-eigenaren en -beheerders om te onthouden dat het niet naleven van deze wetgeving kan leiden tot hoge boetes en reputatieschade. Het is daarom van cruciaal belang om ervoor te zorgen dat de juiste informatie over cookies op de website wordt vermeld en om toestemming te vragen aan gebruikers voordat cookies worden geplaatst.

In het kort

De wetgeving en verplichting van cookies vermelding is een belangrijke stap in het beschermen van de privacy van gebruikers op het internet. Het geeft gebruikers meer controle over hun persoonlijke gegevens en zorgt ervoor dat websites en apps transparant zijn over hun cookiegebruik. Het is belangrijk voor website-eigenaren en -beheerders om de wetgeving en verplichtingen rondom cookies goed te begrijpen en te implementeren, om boetes en reputatieschade te voorkomen.

Naast het voldoen aan de wetgeving is het ook belangrijk om een goede balans te vinden tussen de privacy van gebruikers en het gebruik van cookies om de gebruikerservaring te verbeteren. Websites en apps kunnen bijvoorbeeld alternatieven gebruiken voor het verzamelen van gegevens, zoals het anoniem maken van gegevens, het verminderen van de hoeveelheid verzamelde gegevens of het toestaan van gebruikers om specifieke soorten cookies in of uit te schakelen.

Het is ook belangrijk om gebruikers te informeren over hun rechten en hoe ze hun cookievoorkeuren kunnen beheren. Dit kan bijvoorbeeld worden gedaan door een cookiebeleid op de website te plaatsen en een duidelijke optie te bieden om cookies in of uit te schakelen.

In de huidige digitale wereld is het waarborgen van de privacy van gebruikers cruciaal. Het naleven van de wetgeving en verplichtingen rondom cookies is een belangrijke stap in het beschermen van de privacy van gebruikers en het opbouwen van vertrouwen tussen website-eigenaren en -beheerders en hun gebruikers.

Oh nee, mij wachtwoord is gelekt of ik heb gehackt.

Het is een nare ervaring om het slachtoffer te worden van online oplichting, hacking of ransomware. De gevolgen van dergelijke aanvallen kunnen zeer ernstig zijn, variërend van financiële schade tot reputatieschade en het verlies van persoonlijke gegevens. Het is essentieel om snel te handelen om de schade zoveel mogelijk te beperken en verdere risico's te vermijden. In dit artikel zullen we bespreken wat de mogelijke impact kan zijn, wat je nu moet doen, wat je mogelijks verkeerd deed en wat je kan doen om je in de toekomst te beschermen.

Mogelijke impact

De mogelijke impact van online oplichting, hacking of ransomware is afhankelijk van de aard van de aanval. Hieronder staan enkele voorbeelden van mogelijke gevolgen:

- Financiële schade: De aanvaller kan je bankrekening hacken, creditcardgegevens stelen, of je dwingen om losgeld te betalen om toegang te krijgen tot je bestanden.
- Verlies van persoonlijke gegevens: De aanvaller kan toegang krijgen tot je persoonlijke gegevens, zoals je naam, adres, geboortedatum, e-mailadres en wachtwoorden. Deze informatie kan worden verkocht op de zwarte markt of worden gebruikt voor identiteitsfraude.
- Verlies van belangrijke bestanden: Ransomware kan je bestanden versleutelen, waardoor je geen toegang meer hebt tot belangrijke documenten, foto's of video's.

- Reputatieschade: Als je het slachtoffer wordt van een online oplichter, kan dit je reputatie schaden als anderen ontdekken dat je bent opgelicht.

Wat moet je nu doen?

Als je denkt dat je het slachtoffer bent geworden van online oplichting, hacking of ransomware, zijn hier enkele stappen die je moet ondernemen:

- Verwijder de malware: Als je denkt dat er malware op je computer is geïnstalleerd, moet je deze zo snel mogelijk verwijderen. Gebruik een antivirusprogramma om te scannen op malware en volg de instructies om het te verwijderen. Als je niet zeker weet welk programma je moet gebruiken, helpen wij u graag hierbij.
- Verander je wachtwoorden: Als je denkt dat je wachtwoorden zijn gestolen, moet je ze onmiddellijk wijzigen. Gebruik sterke, unieke wachtwoorden en bewaar ze op een veilige plaats. Maak deze minimaal 13 karakters lang in een combinatie van letters, cijfers, speciale tekens en gebruik niets persoonlijks in uw wachtwoord, zoals naam van familielid, huisdier en zo verder.
- Waarschuw je bank: Als je denkt dat er financiële schade is veroorzaakt, waarschuw dan je bank of creditcardmaatschappij en volg hun instructies op.
- Bewaar bewijsmateriaal: Als je het slachtoffer bent van oplichting, bewaar dan alle bewijsstukken, zoals e-mails, sms-berichten, facturen, etc. Dit kan van pas komen als je later aangifte doet bij de politie.

- Doe aangifte: Als je het slachtoffer bent van oplichting, hacking of ransomware, doe dan aangifte bij de politie. Dit kan helpen bij het opsporen van de daders en het voorkomen van toekomstige incidenten. Doe zeker ook online aangifte op deze website

<https://meldpunt.belgie.be/meldpunt/>

- Controleer je online accounts: Controleer al je online accounts om te zien of er ongebruikelijke activiteiten hebben plaatsgevonden. Als je iets verdachts opmerkt, verander dan onmiddellijk je wachtwoord.

- Maak een back-up van je gegevens: Maak regelmatig een back-up van al je belangrijke gegevens, zodat je deze kunt herstellen als je computer wordt gehackt of geïnfecteerd met ransomware.

Wat deed je mogelijk verkeerd?

Het is belangrijk om te begrijpen wat je mogelijk verkeerd deed, zodat je in de toekomst kunt voorkomen dat je opnieuw het slachtoffer wordt van online oplichting, hacking of ransomware. Enkele veelvoorkomende fouten die mensen maken zijn:

- **Klikken op verdachte links:** Klik nooit op links in e-mails of berichten van onbekende afzenders. Deze links kunnen leiden naar kwaadaardige websites of malware downloaden. Analyseer duidelijk het e-mailadres van de afzender. Hoe je dat doet leren wij u in onze trainingen en voordrachten.
- **Gebruik van zwakke wachtwoorden:** Gebruik nooit eenvoudige wachtwoorden zoals "123456" of "password". Kies in plaats daarvan sterke, unieke wachtwoorden die bestaan uit een combinatie van letters, cijfers en symbolen.
- **Niet bijwerken van software:** Zorg ervoor dat je altijd de nieuwste updates installeert voor je besturingssysteem en andere software die je gebruikt. Deze updates bevatten vaak beveiligingspatches om bekende kwetsbaarheden te dichten.

Wat kan je doen om je in de toekomst te beschermen?

Om jezelf te beschermen tegen online oplichting, hacking en ransomware, zijn hier enkele stappen die je kunt nemen:

- Gebruik antivirussoftware: Installeer antivirussoftware op je computer om te voorkomen dat malware wordt geïnstalleerd. Zorg ervoor dat de software regelmatig wordt bijgewerkt om de nieuwste bedreigingen te detecteren. Niet alle standaard antivirussoftware voldoet, we helpen je graag om je beter te beveiligen met de juiste software.
- Gebruik een firewall: Een firewall kan helpen om ongeautoriseerde toegang tot je computer te voorkomen. Zorg ervoor dat de firewall is ingeschakeld op je computer. Meestal is deze standaard actief maar update deze ook regelmatig.
- Wees voorzichtig met verdachte links: Klik nooit op verdachte links in e-mails of berichten. Controleer altijd de afzender en de URL voordat je op een link klikt. Hoe je dit moet doen leren wij je in onze trainingen en voordrachten.
- Gebruik sterke wachtwoorden: Gebruik sterke, unieke wachtwoorden voor al je online accounts en verander ze regelmatig.
- Maak regelmatig back-ups: Maak regelmatig een back-up van al je belangrijke gegevens. Hierdoor kan je je bestanden herstellen als je computer wordt gehackt of geïnfecteerd met ransomware.

- Wees alert op verdachte activiteiten: Houd je online accounts en bankrekeningen goed in de gaten en wees alert op verdachte activiteiten. Als je iets verdachts opmerkt, neem dan onmiddellijk contact op met je bank of de betreffende website om het probleem te melden.
- Gebruik tweefactorauthenticatie: Schakel tweefactorauthenticatie in voor al je online accounts waarvoor deze functie beschikbaar is. Dit voegt een extra beveiliging laag toe door een extra stap toe te voegen aan het inlogproces, zoals een code die naar je telefoon wordt gestuurd. Ook hier helpen wij u graag bij.
- Wees voorzichtig met openbare wifi: Vermijd het gebruik van openbare wifi- netwerken voor gevoelige activiteiten zoals online bankieren. Deze netwerken zijn vaak onbeveiligd en kunnen je gegevens kwetsbaar maken voor hackers. Doe nooit betalingen of raadpleeg nooit uw bankrekening of andere website die gevoelige informatie bevatten, gebruik hiervoor steeds mobiele data onder 3/4/5G of maak zeker gebruik van een VPN. Meer informatie en het gebruik ervan leren wij u in onze trainingen.
- Wees voorzichtig met downloads: Download nooit software of bestanden van onbetrouwbare bronnen. Deze kunnen malware bevatten die je computer kan infecteren.
- Wees voorzichtig met persoonlijke informatie: Geef nooit persoonlijke informatie zoals je adres, telefoonnummer of financiële gegevens aan onbekende personen of websites. Deze informatie kan worden gebruikt voor identiteitsdiefstal of fraude.

In het geval van online oplichting, hacking of ransomware is het belangrijk om snel en adequaat te handelen om de schade te beperken en verdere incidenten te voorkomen. Het is ook belangrijk om te leren van je fouten en maatregelen te nemen om jezelf in de toekomst te beschermen. Door deze stappen te volgen, kun je jezelf en je gegevens beter beveiligen tegen cyberaanvallen en internetcriminaliteit.

Volg onze trainingen en voordrachten, vraag ons raad om uzelf en uw naasten beter te beschermen tegen de gevaren van het internet.

Internet veiligheid en bewustwording

Het is niet alleen de titel van een van mijn boeken maar ook een leidraad om u bewuster te maken van de gevaren van het internet.

In onze huidige samenleving is het belangrijker dan ooit om op de hoogte te zijn van de risico's en gevaren van het internet. Cybercriminelen worden steeds geavanceerder en maken gebruik van steeds geavanceerdere methoden om toegang te krijgen tot persoonlijke gegevens en systemen. Om jezelf en je organisatie te beschermen tegen deze bedreigingen is het van cruciaal belang om goed geïnformeerd te zijn over cyberveiligheid en de beste praktijken te kennen voor het beveiligen van je gegevens.

Onze Cyber awareness trainingen zijn een effectieve manier om deze kennis en vaardigheden op te doen. Deze trainingen bieden een diepgaand inzicht in de verschillende soorten cyberbedreigingen, waaronder Phishing, malware en ransomware, en geven concrete stappen die je kunt nemen om jezelf en je organisatie te beschermen. Het is een investering in jezelf en je organisatie die zichzelf op lange termijn terugverdient.

Door het volgen van onze cyber awareness trainingen kun je niet alleen je eigen veiligheid verbeteren, maar ook die van je collega's en de organisatie als geheel. Het bevorderen van een cyberbewuste cultuur binnen een organisatie kan helpen om het risico op cyberaanvallen te verminderen en de effectiviteit van de beveiligingsmaatregelen te vergroten.

Bovendien kan het volgen van onze trainingen verplicht zijn voor bepaalde functies of sectoren, zoals bijvoorbeeld in de zorg of bij de overheid. Het is daarom belangrijk om op de hoogte te zijn van de vereisten en ervoor te zorgen dat je de juiste trainingen volgt om aan deze eisen te voldoen.

In het kort: het volgen van onze cyber awareness trainingen zijn essentieel voor iedereen die gebruik maakt van het internet, of je nu een individu bent of een organisatie vertegenwoordigt. Door onze trainingen te volgen, kun je jezelf en anderen beschermen tegen cyberaanvallen en bijdragen aan een veiligere digitale omgeving voor iedereen.

Wat is OSiNT?

OSINT staat voor Open-Source Intelligence en is een inlichtingen- verzamelingstechniek waarmee informatie wordt verzameld over een doelwit, organisatie of gebeurtenis via openbare bronnen. Dit kan informatie zijn die online beschikbaar is, zoals sociale media-profielen, openbare registers, nieuwsartikelen en overheidswebsites.

Deze techniek kan voor verschillende doeleinden worden gebruikt, waaronder beveiligings-onderzoek, spionage, fraudeonderzoek en criminele activiteiten.

Het wordt gebruikt door verschillende instanties, zoals inlichtingendiensten, overheidsinstellingen, rechtshandavingsinstanties, journalisten en bedrijven.

Het is belangrijk op te merken dat het verzamelen van informatie via OSINT ethisch en legaal moet worden uitgevoerd, en dat de privacy van individuen moet worden gerespecteerd. Veel organisaties en bedrijven hebben OSINT- analisten in dienst om deze informatie op een verantwoorde manier te verzamelen en te analyseren.

Hoewel OSINT nuttig kan zijn voor het verzamelen van informatie voor legitieme doeleinden, kan het in de handen van hackers en cybercriminelen ook gevaarlijk zijn.

Het is daarom van essentieel belang om uzelf te beschermen tegen potentiële beveiligingsrisico's door voorzichtig te zijn met uw online informatie en regelmatig uw beveiligingsmaatregelen te controleren en bij te werken.

U dient zich bewust te zijn van de bedreigingen die er zijn en actie te ondernemen om uzelf te beschermen. In de handen van een hacker kan OSINT worden gebruikt om een doelwit te identificeren en informatie over het doelwit te verzamelen. Door verschillende openbare bronnen te onderzoeken, kan een hacker informatie verzamelen over het doelwit, zoals persoonlijke informatie, contactgegevens en zelfs wachtwoorden.

Met deze informatie kan de hacker gerichte aanvallen uitvoeren, zoals social engineering-aanvallen, Phishing-aanvallen, brute-force-aanvallen, fraude en chanteren, en andere vormen van cyberaanvallen. Hackers kunnen verschillende technieken gebruiken om informatie te verzamelen, zoals webscraping, social engineering, Phishing, port scanning en andere methoden.

Om uzelf te beschermen tegen OSINT-gerelateerde bedreigingen, is het belangrijk om sterke wachtwoorden te gebruiken, regelmatig uw online profielen te controleren, en u bewust te zijn van Phishing-aanvallen en andere cyberbedreigingen. Daarnaast moet u uw computer en andere apparaten up- to-date houden met de nieuwste beveiligingsupdates en -patches en indien nodig hulp inroepen van experts op het gebied van cybersecurity.

Inderdaad, het verzamelen van gevoelige informatie via OSiNT kan leiden tot ernstige gevolgen voor individuen en organisaties, zoals financiële verliezen, reputatieschade en zelfs persoonlijke veiligheidsrisico's. Het is daarom van cruciaal belang dat mensen zich bewust zijn van de mogelijke risico's en zich actief inzetten voor het beschermen van hun persoonlijke informatie.

Het nemen van preventieve maatregelen zoals het beperken van de hoeveelheid persoonlijke informatie die online beschikbaar is, het regelmatig controleren van accounts op ongebruikelijke activiteiten en het gebruik van sterke wachtwoorden kan helpen om de veiligheid te verhogen.

Daarnaast is het belangrijk om verdachte activiteiten te melden aan de relevante autoriteiten en om te investeren in beveiligingsmaatregelen zoals firewalls, antivirussoftware en encryptie om de gegevens te beschermen tegen ongeautoriseerde toegang.

Eerste stappen om u te beschermen

Het is belangrijk om alert te blijven bij het delen van informatie online en om verdachte activiteiten of links te vermijden. Het is ook raadzaam om regelmatig back-ups te maken van uw belangrijke gegevens en om te overwegen om encryptie- en beveiligingssoftware te gebruiken om uw gegevens te beschermen. Verder moet u erop letten dat u alleen informatie deelt met betrouwbare en legitieme bronnen en moet u de informatie die u deelt zo veel mogelijk beperken tot wat nodig is.

Het is ook aan te raden om regelmatig uw online activiteiten te controleren om verdachte activiteiten of ongebruikelijke toegang te detecteren. Als u denkt dat uw informatie is gecompromitteerd, moet u onmiddellijk stappen ondernemen om uw accounts te beveiligen en eventuele ongeautoriseerde toegang te blokkeren. Dit kan onder meer het wijzigen van uw wachtwoorden, het informeren van uw bank of creditcardmaatschappij en het melden van de inbreuk bij de relevante instanties omvatten.

Ten slotte moet u zich bewust zijn van de verschillende soorten cyberaanvallen die kunnen worden uitgevoerd met behulp van OSiNT-technieken, zodat u zich beter kunt beschermen tegen deze risico's. Het volgen van het laatste nieuws over beveiligingsproblemen en bedreigingen en het nemen van preventieve maatregelen kunnen helpen om uw online informatie te beschermen en uw persoonlijke gegevens veilig te houden.

Om uzelf te beschermen tegen deze risico's, zijn er verschillende stappen die u kunt nemen.

Ten eerste is het belangrijk om uw online privacy-instellingen te controleren en waar mogelijk te beperken wie toegang heeft tot uw persoonlijke informatie. Dit geldt vooral voor sociale media-profielen en andere onlineaccounts. Zorg ervoor dat uw wachtwoorden sterk zijn en regelmatig worden gewijzigd.

Ten tweede is het belangrijk om alert te blijven bij het delen van informatie online. Wees voorzichtig met het delen van persoonlijke informatie, vooral als u niet bekend bent met de persoon of het bedrijf waarmee u communiceert. Vermijd ook het klikken op verdachte links of het downloaden van bestanden van onbekende bronnen.

Tot slot is het belangrijk om up-to-date te blijven over beveiligingsproblemen en bedreigingen, zodat u zichzelf kunt beschermen tegen potentiële aanvallen. Dit omvat het volgen van het laatste nieuws op het gebied van beveiliging, het updaten van uw software en het gebruik van antivirus- en firewallprogramma's.

Als u zich zorgen maakt over de beveiliging van uw online informatie, zijn er verschillende maatregelen die u kunt nemen om uzelf te beschermen. Ten eerste moet u uw online privacy-instellingen controleren en waar mogelijk beperken wie toegang heeft tot uw persoonlijke informatie. U kunt ook overwegen om sterke wachtwoorden te gebruiken en regelmatig uw wachtwoorden te wijzigen.

Een belangrijk onderdeel van het beschermen van uzelf tegen OSiNT-gerelateerde bedreigingen is het begrijpen van hoe hackers informatie verzamelen en wat voor soort informatie zij zoeken.

Hackers zullen bijvoorbeeld vaak zoeken naar informatie over uw online activiteiten, zoals de websites die u bezoekt, uw zoekgeschiedenis en uw sociale media-profielen. Zij kunnen ook proberen uw fysieke locatie te achterhalen, bijvoorbeeld door gebruik te maken van informatie over uw IP-adres of mobiele telefoon.

Om te voorkomen dat hackers deze informatie kunnen verzamelen, kunt u een aantal maatregelen nemen.
Bijvoorbeeld:

- Gebruik VPN-software om uw IP-adres te verbergen en uw internetverkeer te versleutelen.
- Gebruik privacy vriendelijke zoekmachines zoals DuckDuckGo in plaats van Google, die uw zoekgeschiedenis niet opslaat en u dus beter beschermt tegen tracking.
- Beperk de informatie die u deelt op sociale media-profielen en controleer uw privacy-instellingen zodat alleen mensen die u kent toegang hebben tot uw informatie.
- Gebruik sterke wachtwoorden
- Schakel tweestapsverificatie in waar mogelijk om uw accounts te beschermen.
- Wees voorzichtig met het openen van links en het downloaden van bijlagen van onbekende afzenders op social media.

Door deze maatregelen te nemen, kunt u uzelf beschermen tegen de risico's van OSiNT en social media. Het is belangrijk om bewust te zijn van de informatie die u deelt op social media en om regelmatig uw beveiligingsmaatregelen bij te werken om uzelf te beschermen tegen de steeds evoluerende dreiging van cybercriminaliteit.

Als u denkt dat u het slachtoffer bent geworden van een OSiNT-gerelateerde aanval, is het belangrijk om snel te handelen. U kunt bijvoorbeeld uw wachtwoorden wijzigen en uw accounts controleren op ongebruikelijke activiteiten. U kunt ook contact opnemen met de relevante instanties, zoals de politie of een cybersecurity-bedrijf, voor verdere ondersteuning. Al blijkt dit in de praktijk een lachertje te zijn.

Kortom, OSiNT kan zeer nuttig zijn voor het verzamelen van informatie voor legitieme doeleinden, maar het kan ook een bedreiging vormen in de handen van hackers en cybercriminelen. Het is belangrijk om uzelf te beschermen tegen potentiële beveiligingsrisico's door uw online informatie zorgvuldig te beheren en regelmatig uw beveiligingsmaatregelen bij te werken. Door alert te blijven en snel te handelen als u denkt dat u het slachtoffer bent geworden van een aanval, kunt u uzelf beschermen tegen de risico's van OSiNT.

OSiNT en Social Media

OSiNT staat voor Open-Source Intelligence, wat inhoudt dat het gebruikmaakt van openbaar beschikbare informatie om inzicht te krijgen in een persoon, bedrijf of organisatie. In de moderne tijd wordt OSiNT vaak geassocieerd met het gebruik van social media, aangezien deze platforms een overvloed aan informatie bieden over individuen en organisaties.

Social media kan een waardevolle bron van informatie zijn voor OSiNT- onderzoekers. Deze platforms bieden vaak informatie over de interesses, vriendenkring, locaties en activiteiten van individuen, en bieden ook mogelijkheden om contact te leggen en communicatie te volgen. Dit kan bijvoorbeeld handig zijn voor bedrijven die marktonderzoek willen doen, of voor overheidsinstanties die informatie willen verzamelen over potentiële bedreigingen voor de nationale veiligheid.

Het gebruik van social media voor OSiNT brengt ook bepaalde risico's met zich mee. Hackers en cybercriminelen maken vaak gebruik van social media om persoonlijke informatie te verzamelen over hun slachtoffers, zoals e- mailadressen, wachtwoorden en andere gevoelige informatie. Deze informatie kan worden gebruikt voor identiteitsdiefstal, Phishing-aanvallen en andere vormen van cybercriminaliteit.

Bovendien kan het delen van persoonlijke informatie op social media leiden tot privacy- en beveiligingsrisico's. Veel mensen delen onbewust te veel informatie op social media, zoals hun volledige naam, geboortedatum, adres, werkgever en andere gevoelige gegevens. Dit maakt het gemakkelijker voor hackers en andere kwaadwillende om persoonlijke informatie te verzamelen en te misbruiken.

OSiNT in het echte leven – test jezelf

Stel we nemen Facebook als voorbeeld. Vraag aan een bevriend iemand om uw profiel te bezoeken, en geef een onbekende uw gsm of pc en laat deze gewoon naar uw profiel kijken.

In 80% van de gevallen ziet deze al uw andere vrienden, in 50% van de gevallen uw geboortjaar, geboorteplaats, bijna 99% een profielfoto van u, en denk dan even na wat een kwaadwillend persoon hiermee al kan aanvangen. In 50% van de gevallen ziet deze ook al uw interesses, wat u graag of niet graag hebt, om maar te zwijgen over de pagina en/of groepen die u volgt. Erger nog, misschien schreef u zelfs ‘in verlov van Tot’.

Vraag nu aan een niet bevriende persoon uw profiel te bekijken, met deze mindset, u wilt alles over jezelf (doelwit) weten. Al uw vrienden, wie u moeder, vader, broer, zuster, nonkel enzo is. U interesses, gelezen boeken, bezochte plaatsen en zo verder. Wat u net deed is maar een fractie van wat OSiNT is, maar bekijk en zie wat een onbekende al over u weet. Als deze dan nog eens “vriend” met u kan worden, ja dan.

Waartoe kan al deze informatie leiden? We gaan hier nu niet verder op in, maar uiteindelijk is ieder wachtwoord te kraken over tijd, echter als men al heel wat persoonlijke informatie van u kan vinden online, en wetende dat 80 % van de mensen persoonlijke informatie gebruikt in zij wachtwoord dan is het al heel stuk makkelijker om u wachtwoord te kraken.

We gaan het hier dan nog niet hebben over de mensen die geen hackers zijn maar uit zijn op “vriendschap-fraude”. Bevriend worden, online een relatie faken, en dan plots met een foefje een klein geldbedrag vragen, totaal onschuldig maar de eerste stap in een reeks van.

Of u ontvang plots een sms, zagezegd van een familielid (met naam en toenaam, niet moeilijk te vinden, u deelde dit zelf op social Media, met een of ander soms heel geloofwaardig verhaal om geld te vragen.

Dit is een heel klein stukje maar van wat OSiNT in de verkeerde handen kan doen. In onze voordrachten en trainingen gaan we daar veel dieper op in en veelal zie je toeschouwers groen lachen. En terecht. Vergeet niet dat bij een online oplichting u zo goed als zeker hebt meegewerkt, misschien te goeder trouw maar u hebt mee er schuld aan. Harde woorden weet ik maar het is zo.

OSiNT en het world-wide-web

Het internet is een belangrijke bron van informatie voor OSiNT-onderzoekers, omdat vrijwel alles wat online wordt gepubliceerd openbaar toegankelijk is.

Wanneer u een website bezoekt, geeft u onbewust veel informatieprijs aan de eigenaar van de website. Zo kan de eigenaar van de website bijvoorbeeld uw IP-adres, de browser die u gebruikt, het besturingssysteem dat u gebruikt, uw locatie en zelfs uw zoekgeschiedenis op de website bijhouden. Deze informatie kan worden gebruikt om uw online activiteiten te volgen en te monitoren.

Bovendien kan informatie op websites worden gebruikt om een beeld te vormen van personen, bedrijven of organisaties. Zo kunnen sociale media- profielen worden gekoppeld aan websites, waardoor er meer informatie beschikbaar komt over de interesses, voorkeuren en activiteiten van individuen. Bedrijfswebsites kunnen informatie bevatten over producten, diensten en werknemers, wat kan helpen bij marktonderzoek of concurrentieanalyse.

Het is echter belangrijk om op te merken dat niet alle informatie op websites betrouwbaar is. Het internet staat vol met valse informatie, nepnieuws en desinformatie, en het is aan de OSiNT-onderzoeker om de betrouwbaarheid van de informatie te beoordelen voordat deze wordt gebruikt in een onderzoek. Om uzelf te beschermen tegen de risico's van OSINT en websites, zijn er verschillende maatregelen die u kunt nemen.

Bijvoorbeeld:

- Gebruik een VPN om uw IP-adres te verbergen en uw online activiteiten te beschermen tegen monitoring en tracking.
- Gebruik een adblocker om ongewenste advertenties en pop-ups te blokkeren, wat kan helpen om de veiligheid van uw computer te waarborgen.
- Gebruik antivirussoftware om uw computer te beschermen tegen malware en andere cyberbedreigingen die kunnen worden verspreid via websites.
- Controleer de betrouwbaarheid van de informatie op websites voordat u deze gebruikt in een onderzoek. Verifieer de informatie met andere bronnen en beoordeel de kwaliteit van de bron.

Naast de informatie die u onbewust prijsgeeft wanneer u een website bezoekt, zijn er ook andere manieren waarop websites informatie kunnen verzamelen over u. Bijvoorbeeld via cookies en trackers.

Cookies zijn kleine tekstbestanden die door websites op uw computer worden geplaatst om uw voorkeuren te onthouden en uw online ervaring te verbeteren.

Trackers zijn scripts die worden gebruikt om uw online activiteiten te volgen en te rapporteren aan derden, zoals adverteerders en analysebedrijven.

Hoewel cookies en trackers vaak worden gebruikt om uw online ervaring te verbeteren, kunnen ze ook worden gebruikt om uw privacy te schenden en uw online activiteiten te volgen en te monitoren. Het is daarom belangrijk om cookies en trackers te beheren en alleen de essentiële cookies toe te staan.

Daarnaast is het belangrijk om te weten dat niet alle websites veilig zijn. Sommige websites zijn ontworpen om uw computer te infecteren met malware of om uw persoonlijke gegevens te stelen. Het is daarom belangrijk om alleen websites te bezoeken die u vertrouwt en om uw beveiligingsmaatregelen bij te werken om uzelf te beschermen tegen cybercriminaliteit.

Tot slot kan OSiNT-onderzoek een krachtig hulpmiddel zijn voor bedrijven, overheden en andere organisaties om inzicht te krijgen in personen, bedrijven en andere entiteiten. Het is echter belangrijk om de risico's en uitdagingen van OSiNT te begrijpen, zoals het risico op het verzamelen van valse of misleidende informatie. Door bewust te zijn van deze risico's en maatregelen te nemen om uzelf te beschermen, kunt u optimaal gebruik maken van de voordelen van OSiNT zonder uw privacy en veiligheid in gevaar te brengen.

We hebben een webpagina aangemaakt om u een praktisch beeld te geven van alle data die vrij ter beschikking stelt zonder uw medeweten en die zoals eerder vermeld positief maar eventueel ook negatief kan gebruik worden.

<https://ethisch-hacker.be/osint/>

Op deze pagina ziet u al heel wat informatie omtrent uzelf. Dit is informatie die u deelt, eigenlijk zonder u mede weten, aan de eigenaar van de website. Dit kan nuttig zijn voor commerciële doeleinden, bvb om na te gaan van waar uw bezoeker komen, binnen of buiten uw stad of provincie, of internationaal. Heb u veel bezoekers die Windows, Mac of andere systemen gebruiken, zijn de meeste mobile of vaste pc-gebruikers enzo.

Net zoals vele dingen kan deze informatie ook verkeerdelijk gebruik worden door kwaadwillende personen.

Wat kan u doen?

Een aantal van deze gegevens kan u beïnvloeden, zoals uw locatie, zelfs welk type PC of Mac u gebruikt, maar de meeste voorkomende en eigenlijk eenvoudigste manier is;

Gebruik een VPN om uw IP-adres te verbergen en uw online activiteiten te beschermen tegen monitoring en tracking.

Wat is een VPN nu juist?

Een VPN (Virtual Private Network) is een technologie die steeds populairder wordt onder internetgebruikers over de hele wereld. Het is een veilige en betrouwbare manier om internetverkeer te versleutelen en het te beschermen tegen nieuwsgierige blikken en cyberaanvallen.

Een van de belangrijkste redenen om een VPN te gebruiken, is om uw privacy te beschermen. Door uw internetverbinding te versleutelen, voorkomt u dat derden, zoals uw internetprovider of hackers, toegang krijgen tot uw gevoelige gegevens en online activiteiten. Bovendien kan een VPN u helpen uw locatie te verbergen en uw anonimiteit te behouden.

Een ander belangrijk voordeel van een VPN is dat het uw online veiligheid verhoogt. Door uw internetverbinding te versleutelen, kunt u voorkomen dat cybercriminelen uw gegevens stelen en uw apparaten infecteren met malware en virussen. Daarnaast kunt u met een VPN veilig en anoniem bestanden delen en downloaden, zonder dat u zich zorgen hoeft te maken over juridische gevolgen of boetes. Kanttekening: zoals u dus merkt kan een VPN ook “verkeerdelijk” gebruikt worden.

Kortom, een VPN is een essentieel hulpmiddel geworden voor internetgebruikers die hun privacy en veiligheid serieus nemen. Of u nu een zakelijke professional bent die vaak onderweg is, een student die in een studentenhuis woont of gewoon iemand die graag veilig en anoniem online wil zijn, een VPN kan u helpen uw internetervaring te verbeteren en uw gegevens te beschermen tegen nieuwsgierige blikken en cyberbedreigingen.

Gebruik een adblocker om ongewenste advertenties en pop-ups te blokkeren, wat kan helpen om de veiligheid van uw computer te waarborgen.

En een adblocker is?

Een adblocker is een nuttig hulpmiddel voor het blokkeren van advertenties tijdens het browsen op internet. Het is een browserextensie die u kunt installeren om advertenties en pop-ups te blokkeren die anders uw surfervaring kunnen verstoren. Het gebruik van een adblocker biedt verschillende voordelen.

Ten eerste vermindert het de afleiding en irritatie veroorzaakt door advertenties die uw scherm overnemen. Dit kan leiden tot een verbeterde surfervaring en meer focus op de inhoud die u daadwerkelijk wilt zien.

Ten tweede kan het gebruik van een adblocker ook de laadtijd van webpagina's verbeteren, omdat advertenties vaak grote bestanden zijn die de pagina vertragen. Dit kan resulteren in een snellere, meer responsieve internetervaring.

Een ander voordeel van het gebruik van een adblocker is dat het uw privacy en beveiliging kan beschermen. Advertenties kunnen worden gebruikt om uw online activiteiten bij te houden en persoonlijke informatie te verzamelen, en soms bevatten ze zelfs kwaadaardige code die uw apparaat kan infecteren. Een adblocker kan deze bedreigingen helpen blokkeren en uw gegevens beschermen.

Het is belangrijk op te merken dat het gebruik van een adblocker een nadelig effect kan hebben op de inkomsten van websites en uitgevers die afhankelijk zijn van advertenties voor hun inkomsten. Als u echter merkt dat advertenties uw surfervaring verstoren of uw privacy en veiligheid in gevaar brengen, kan het gebruik van een adblocker een nuttige oplossing zijn.

Ook hier weer een kanttekening: Sommige websites werken niet of slecht wanneer zij een adblocker detecteren.

Wat is een tracker?

Een tracker is een stukje code dat op een website wordt geplaatst om het gedrag van gebruikers te volgen en te analyseren. Dit kan gebruikt worden voor verschillende doeleinden, zoals het bijhouden van welke pagina's een gebruiker bezoekt, hoelang ze op een pagina blijven, welke links ze aanklikken, enzovoorts. Door deze gegevens te verzamelen, kunnen bedrijven en adverteerders een beter inzicht krijgen in het gedrag van hun websitebezoekers en hun marketinginspanningen beter afstemmen op hun doelgroep.

Een veelgebruikte tracker is de Facebook Pixel. Dit is een stukje code dat op een website wordt geplaatst om het gedrag van gebruikers te volgen en te analyseren, en om adverteerders in staat te stellen de effectiviteit van hun advertenties op Facebook te meten.

Met de Facebook Pixel kunnen adverteerders bijvoorbeeld zien hoeveel mensen doorklikken naar hun website vanuit een Facebook-advertentie en welke acties deze gebruikers op de website ondernemen, zoals het doen van een aankoop of het invullen van een contactformulier.

Hoewel het voor adverteerders handig kan zijn om deze gegevens te verzamelen, kan het voor gebruikers ook als indringend worden ervaren omdat hun onlineactiviteiten worden bijgehouden. Het is daarom belangrijk om op de hoogte te zijn van welke trackers er op een website staan en hoe ze worden gebruikt, zodat je bewuste keuzes kunt maken over je online privacy. Gelukkig bieden veel browsers en browserextensies de mogelijkheid om trackers te blokkeren of te beperken, zodat je meer controle hebt over welke gegevens er worden verzameld.

Hier wordt het eigenlijk wel leuk want bvb Google beschuldigd Facebook zo van inbreuk op de privacy en "spionage" terwijl ze zelf ook dergelijk systeem gebruiken. Apple bvb legt de laatste jaren enorm nadruk op privacy en wil Facebook en Google zo zelf weren van hun Appleproducten maar zelf doen ze het ook.

Bewijs ervan zien?

Bekijk dan even naar een video via YouTube

<https://www.youtube.com/watch?v=jign96jk0s4>

Zoals u merkt kunt u heel wat doen om uzelf te beschermen en iets meer privacy te verkrijgen op het internet. Kan je alles vermijden nee, moeilijk maken wel. Daarom is het ook zo moeilijk om bvb de locatie van een hacker terug te vinden bij fraude of oplichting. Er moeten daarvoor een gans aantal organisaties samenwerken, wat in de praktijk heel moeilijk ligt.

Nogmaals, en ik weet het zijn hard woorden, maar bent u opgelicht dan hebt u daar een stukje eigen schuld in, door geweld of onbewust uw medewerking te hebben gegeven.

Hackers gaan steeds sluwer en “vertrouwelijker” te werk om uw gegevens te ontfutselen.

In dit boek hebben wij een stukje van de sluimer maar opgelicht, er zijn heel wat technieken en mogelijkheden om informatie omtrent een doelwit te verzamelen, en dit alles op een legale manier.

Ik hoop dat u wat hebt opgestoken van deze informatie.

Bonus tip

Op uw thuis PC/ Mac draait u een e-mail client (outlook of ander), er is de mogelijkheid om meegestuurde foto's (logo en andere (zoals tracker)) te verbergen bij het openen van de e-mail, activeer deze optie. Wij ontwikkelden een soort tracker die eigenlijk een foto is van 1pixel op 1pixel transparant groot. Door afbeeldingen bij het laden uit te schakelen wordt dus ook de tracker niet geladen. Wij ontwikkelden deze om bvb een overzicht te geven van

het aantal dagelijkse terugkerende of unieke bezoekers en of ze van de streek zijn.

Sommige bedrijven vonden een systeem uit waarbij hun tekst in een foto formaat staat en u dus niets ziet tenzij u de afbeelding toelaat in te laden, wees dan maar zeker dat u een tracker activeerde.

QR-codes zijn overal.

We gebruiken ze om:

- Websites te openen,
- Apps te downloaden,
- Loyalteitspunten te verzamelen,
- Betalingen te doen
- Geld over te maken.
-

De technologie is handig, waardoor ook cybercriminelen er graag gebruik van maken. Een trend is dat cybercriminelen QR-codes aanmaken en deze verspreiden. Op deze manier kunnen ze hun slachtoffers doorverwijzen naar dubieuze websites of applicaties en proberen ze gevoelige gegevens te bemachtigen, malware op uw telefoon te installeren of u over te halen om een betaling te doen. Cybercriminelen moeten hun slachtoffers dus eerst overtuigen om de kwaadaardige QR-code te scannen en erop te klikken of te tikken. Ze gebruiken hiervoor verschillende tactieken.

Reputatie van legitieme partijen

Vaak misbruiken cybercriminelen het werk en de reputatie van legitieme partijen. Ze vervangen bijvoorbeeld een QR-code op een poster of menukaart door een kwaadaardige code. Zodra een gebruiker de code scant en vervolgens op de link klikt, komt hij of zij terecht op een Phishing-site die veel weg heeft van een inlogpagina van een sociaal netwerk of online-bank. Op deze manier ontfutselen ze gevoelige informatie, zoals wachtwoorden of bankgegevens. Vaak plaatsen ze ook banners met een kwaadaardige QR-code of versturen ze e-mails die verwijzen naar een kwaadaardige QR-code.

Cybercriminelen laten QR-codes soms bepaalde acties uitvoeren. Zodra een slachtoffer de code scant, belt hij of zij automatisch een telefoonnummer tegen betaling. Een andere tactiek is de babbeltruc.

De gedupeerden worden op straat aangesproken en gevraagd om via een QR-code geld over te maken voor de parkeerautomaat, omdat de cybercriminelen zelf alleen cash bij zich hebben. Om het geld over te maken, moet het slachtoffer even een code scannen. Vervolgens belandt het slachtoffer op een nep-site met een inlogprocedure. De oplichter heeft vervolgens toegang tot de bankrekening van het slachtoffer, met alle gevolgen van dien.

De mogelijkheden zijn eindeloos voor cybercriminelen. Kwaadaardige QR-codes worden aangetroffen op rekeningen, pamfletten, in presentaties en vrijwel overal waar informatie of instructies worden verwacht.

Wat kun je doen om te voorkomen dat je per ongeluk een kwaadaardige code scant?

Naast het controleren van de link, zijn er nog andere maatregelen die je kunt nemen om te voorkomen dat je per ongeluk een kwaadaardige code scant.

Hieronder staan enkele tips:

- Gebruik een betrouwbare antivirus- en anti-malware software op je apparaat. Dit kan helpen om kwaadaardige software te detecteren en te verwijderen.
- Vermijd het scannen van codes van onbekende bronnen of van codes die ongevraagd zijn ontvangen.
- Wees voorzichtig bij het scannen van codes die beloven om te helpen bij het winnen van prijzen, gratis abonnementen of andere aanbiedingen die te mooi lijken om waar te zijn.
- Gebruik een QR-code scanner van een betrouwbare bron, bijvoorbeeld van een gerenommeerde app store.
- Als je twijfelt over de echtheid van een code, vraag dan aan de uitgever van de code om bevestiging of neem contact op met de klantenservice van het betreffende bedrijf.

Het is belangrijk om te onthouden dat kwaadaardige codes steeds geavanceerder worden en dat er geen garantie is dat je altijd veilig bent, zelfs als je alle voorzorgsmaatregelen neemt. Het is daarom belangrijk om alert te blijven en verdachte activiteiten onmiddellijk te melden.

Het is een goede gewoonte goed te letten op de link die verschijnt na het scannen van de code. Als je met een smartphone de camera op de QR-code richt, zal de telefoon voorstellen de link te openen, vervolgens kun je de link controleren.

Ziet deze er vreemd uit, klik dan niet op de link. Soms is de link ingekort, wees dan extra voorzichtig want met QR-codes is er geen reden om een link in te korten. Gebruik in plaats daarvan een zoekmachine of ga zelf naar de officiële winkel of het online-adres.

Indien een code op een poster staat, is het verstandig een snelle 'fysieke' controle uit te voeren. Het kan namelijk voorkomen dat een kwaadaardige code over de originele code is geplakt.

"Alertheid vormt nog altijd het beste wapen om je te beschermen tegen cybercriminelen"

Als je er zeker van wilt zijn dat de QR-code veilig is, doe je er verstandig aan om een speciale scanner te gebruiken die de code controleert op schadelijke inhoud en valse (Phishing)websites.

Daarnaast vormt alertheid nog altijd het beste wapen om je te beschermen tegen cybercriminelen. Als iemand je op straat vraagt een QR-code wil scannen, dan kan dit potentieel gevaarlijk zijn. Oplichters zijn goed in het misbruiken van behulpzame mensen.

Ze doen vaak alsof ze haast hebben, waardoor je geen tijd hebt om na te denken. Voel je daarom niet schuldig om gewoon weg te lopen als je het niet vertrouwt. Ook als je twijfelt aan de authenticiteit van een QR-code op een folder, is het over het algemeen verstandiger om de code niet te scannen. Het is misschien langzamer, maar je kunt altijd handmatig naar de website gaan voor meer informatie.

Mocht je nu toch slachtoffer zijn geworden, doe dan altijd aangifte bij de politie. Dit kan eenvoudig online via het meldpunt voor internet fraude (BE).

<https://meldpunt.belgie.be/meldpunt/>

Vaak doen slachtoffers dit niet. Maar met het bewijsmateriaal kunnen de politiediensten onderzoek doen naar de daders. Alle aangiftes samen geven inzicht in hoe cybercriminelen handelen. Hoe meer informatie, hoe groter de kans dat het onderzoek succesvol is. Met jouw aangifte help je dus ook andere slachtoffers. Ook maken de aangiftes het mogelijk nieuwe vormen van cybercrime te herkennen en beveiligingssoftware en systemen erop aan te passen.

Hoewel QR-codes eenvoudig in gebruik zijn en veel mogelijkheden bieden, is het belangrijk om alert te blijven. Veiligheid en gemak gaan immers niet hand in hand. Denk dus twee keer na voordat je een QR-code gebruikt.

Wat zijn beacons?

Beacons zijn kleine, draadloze apparaten die signalen uitzenden via Bluetooth Low Energy (BLE) naar andere apparaten die zich in de buurt bevinden. Dit maakt het mogelijk om op korte afstand te communiceren met apparaten zoals smartphones of tablets. Beacons kunnen op verschillende manieren worden ingezet, bijvoorbeeld in winkels, op evenementen, in musea of op andere locaties waar het belangrijk is om relevante informatie te verstrekken aan gebruikers. Deze signalen kunnen worden gebruikt om locatie gebaseerde diensten aan te bieden aan gebruikers, zoals het verstrekken van informatie over nabijgelegen producten, promoties of andere relevante informatie. In dit artikel zullen we dieper ingaan op beacons, hun gebruiksmogelijkheden, de gevaren en hoe ze mensen kunnen volgen.

iBeacon is een specifieke vorm van een beacon, ontwikkeld door Apple. Het maakt gebruik van Bluetooth Low Energy (BLE) technologie om signalen uit te zenden die worden opgevangen door Apple-apparaten, zoals de iPhone en de iPad. Hierdoor kan het apparaat worden gelokaliseerd en kan er gerichte informatie worden verstrekt aan de gebruiker.

Wat zijn de mogelijkheden van beacons?

Beacons hebben tal van mogelijkheden en kunnen op verschillende manieren worden ingezet. Hieronder staan enkele voorbeelden:

- Retail: Beacons kunnen worden gebruikt om winkelervaringen te verbeteren. Door beacons in de winkel te plaatsen, kunnen klanten bijvoorbeeld aanbiedingen en promoties ontvangen die relevant zijn voor de producten die ze bekijken. Beacons kunnen ook worden gebruikt om klanten te helpen bij het vinden van specifieke producten in de winkel.
- Evenementen: Beacons kunnen worden ingezet bij evenementen, zoals concerten, sportevenementen of conferenties. Hierdoor kunnen deelnemers informatie ontvangen over programma's, locaties en andere belangrijke informatie.
- Musea: Beacons kunnen worden gebruikt om interactieve rondleidingen te bieden in musea. Door beacons te plaatsen bij verschillende tentoonstellingen, kunnen bezoekers informatie ontvangen over de tentoonstelling die ze bekijken.
- Gezondheidszorg: Beacons kunnen worden ingezet in de gezondheidszorg, bijvoorbeeld om patiënten te helpen bij het navigeren door het ziekenhuis of om artsen en verpleegkundigen te helpen bij het volgen van de locatie van medische apparatuur.

Wat zijn de gevaren van beacons?

Hoewel beacons tal van mogelijkheden bieden, zijn er ook enkele potentiële gevaren aan verbonden. Hieronder staan enkele voorbeelden:

- **Privacy:** Beacons kunnen worden gebruikt om de locatie van gebruikers te volgen, wat een bedreiging kan vormen voor de privacy van gebruikers. Bijvoorbeeld, wanneer beacons worden ingezet in winkels, kunnen retailers de locatie van klanten volgen en deze informatie gebruiken om gerichte marketingcampagnes op te zetten. Beacons kunnen een privacy risico vormen als ze worden gebruikt om de locatie van gebruikers te volgen zonder hun toestemming of als de informatie die wordt verzameld wordt gebruikt voor doeleinden die niet in overeenstemming zijn met de privacywetgeving.
- **Veiligheid:** Beacons kunnen ook een veiligheidsrisico vormen, vooral als ze niet goed worden beveiligd. Hackers kunnen bijvoorbeeld een vals signaal uitzenden dat lijkt op een beacon-signaal, wat kan leiden tot verwarring bij gebruikers en hen kan blootstellen aan risico's.
- **Afhankelijkheid van technologie:** Het gebruik van beacons kan leiden tot afhankelijkheid van technologie. Wanneer beacons bijvoorbeeld worden gebruikt om informatie te verstrekken aan bezoekers van een museum, kan dit ervoor zorgen dat bezoekers minder aandacht hebben voor de tentoonstelling zelf en meer bezig zijn met hun smartphone. Het gebruik van beacons vereist dat gebruikers hun Bluetooth ingeschakeld hebben en een app hebben gedownload die in staat is om de signalen van de beacon te ontvangen.

Dit kan leiden tot afhankelijkheid van technologie en kan een uitdaging vormen voor gebruikers die geen toegang hebben tot de benodigde apparaten of apps.

- Kosten: Het opzetten en onderhouden van een beacon-systeem kan een aanzienlijke investering vereisen, vooral voor kleinere bedrijven en organisaties.

Hoe kunnen beacons mensen volgen?

Beacons kunnen worden gebruikt om de locatie van apparaten en daarmee de locatie van gebruikers te volgen. Wanneer een gebruiker een locatie met beacons betreedt, zal het apparaat het signaal van de beacons oppikken en de locatie van de gebruiker registreren.

Door het aantal beacons en de locatie van de beacons te combineren, kan de exacte locatie van een gebruiker worden bepaald.

Hoewel dit potentieel handig kan zijn voor locatie gebaseerde diensten, kan het ook zorgen voor privacy- en veiligheidsrisico's. Bedrijven kunnen de locatie van klanten volgen en deze informatie gebruiken om gerichte marketingcampagnes op te zetten. Bovendien kunnen hackers een vals signaal uitzenden dat lijkt op een beacon-signaal, waardoor gebruikers worden blootgesteld aan risico's.

Welke type beacons bestaan er?

Er bestaan verschillende soorten beacons die elk op hun eigen manier werken en voor verschillende doeleinden kunnen worden gebruikt. Hieronder vind je een overzicht van de meest voorkomende typen beacons:

- Bluetooth Low Energy (BLE) beacons: Dit is de meest gebruikte en bekende vorm van beacons. BLE beacons werken met de Bluetooth Low Energy technologie en hebben een bereik van enkele tientallen meters. Ze worden vaak gebruikt voor locatie gebaseerde diensten in winkels, musea, evenementen en op andere locaties waar informatie aan gebruikers moet worden verstrekt.
- Wi-Fi beacons: Wi-Fi beacons werken met Wi-Fi technologie en hebben een groter bereik dan BLE beacons. Ze worden vaak gebruikt in grote ruimtes zoals winkelcentra, luchthavens en treinstations.
- Ultrasone beacons: Ultrasone beacons werken met geluidsgolven die voor het menselijk oor niet waarneembaar zijn. Ze worden vaak gebruikt in combinatie met een smartphone-app om gebruikers op basis van hun locatie gerichte advertenties te tonen.
- GPS-beacons: GPS-beacons werken met GPS-technologie en hebben een groot bereik. Ze worden voornamelijk gebruikt voor outdoor tracking en navigatie, bijvoorbeeld om wandelroutes te volgen.

- NFC-beacons: NFC-beacons werken met Near Field Communication (NFC) technologie en worden vaak gebruikt voor mobiele betalingen en het verstrekken van informatie aan gebruikers op korte afstand.

Elk type beacon heeft zijn eigen kenmerken en voordelen, afhankelijk van het doel waarvoor het wordt gebruikt. Bij het kiezen van het juiste type beacon is het daarom belangrijk om rekening te houden met het beoogde doel en de specifieke eisen en beperkingen van de omgeving waarin het wordt gebruikt.

Hoe werkt een beacon?

Een beacon zendt een uniek signaal uit dat kan worden opgevangen door een smartphone of ander apparaat met Bluetooth ingeschakeld. Dit signaal bevat informatie zoals de identiteit van de beacon en de locatie waar deze zich bevindt. Wanneer een apparaat het signaal van een beacon ontvangt, kan het de locatie van de gebruiker bepalen en gepersonaliseerde informatie leveren op basis van die locatie.

Om een beacon te kunnen gebruiken, moet de gebruiker eerst een app downloaden die in staat is om de signalen van de beacon te ontvangen en te interpreteren. Wanneer de app het signaal van een beacon oppikt, kan deze informatie gebruiken om specifieke acties uit te voeren, zoals het verstrekken van informatie, het starten van een app of het aanbieden van een korting bon.

Wat zijn de voordelen van beacons?

- Personalisatie: Beacons maken het mogelijk om gebruikers gepersonaliseerde informatie te leveren op basis van hun locatie en voorkeuren. Dit kan leiden tot een betere gebruikerservaring en meer betrokkenheid van gebruikers.
- Efficiëntie: Beacons kunnen informatie leveren aan gebruikers op het juiste moment en op de juiste plaats, waardoor ze tijd besparen en de gebruikerservaring verbeteren.
- Klantbetrokkenheid: Beacons kunnen worden gebruikt om klanten te betrekken bij het merk of de organisatie door hen relevante informatie te verstrekken en hen te belonen voor hun loyaliteit.
- Analyse: Beacons maken het mogelijk om gegevens te verzamelen over het gedrag van gebruikers en hun voorkeuren, waardoor bedrijven en organisaties beter in staat zijn om hun aanbod af te stemmen op de behoeften van hun klanten.

Beacons in de praktijk.

Tijdens mijn recente bezoek aan een ziekenhuis, om privacy redenen kan ik de naam niet noemen, viel het me op dat beacons werden gebruikt. Hoewel ik geen bevestiging kan geven alle ziekenhuizen daadwerkelijk beacons hebben geïmplementeerd, ben ik er vrij zeker van dat andere ziekenhuizen in de toekomst ook overwegen om deze technologie te gebruiken.

Hoe werkt het volgen van aanwezigheid met beacons?

Om aanwezigheid te volgen, plaatst men beacons in de ruimte die men wil bewaken. Wanneer een smartphone of ander apparaat met een compatibele app in de buurt van een beacon komt, ontvangt het apparaat een signaal van de beacon. De app kan deze signalen gebruiken om te bepalen waar het apparaat zich bevindt en om de aanwezigheid van mensen in de ruimte te volgen.

Het volgen van aanwezigheid met beacons kan op verschillende manieren worden gedaan, afhankelijk van de behoeften van de gebruiker. Een van de meest voorkomende methoden is het tellen van het aantal signalen dat wordt ontvangen door een apparaat. Wanneer een apparaat bijvoorbeeld een signaal van een beacon ontvangt, wordt dit beschouwd als een aanwezigheid in de buurt van die beacon. Door het aantal signalen te tellen dat een apparaat ontvangt, kan worden bepaald hoeveel mensen zich in een bepaalde ruimte bevinden.

Waarom is het nuttig om aanwezigheid te volgen met beacons?

Het volgen van aanwezigheid met beacons kan nuttig zijn voor verschillende toepassingen, waaronder:

- **Veiligheid en beveiliging:** Door de aanwezigheid van mensen in een ruimte te volgen, kunnen beacons worden gebruikt om ervoor te zorgen dat niemand ongeoorloofd toegang heeft tot beveiligde gebieden. Ze kunnen ook worden gebruikt om te bepalen of mensen zich op een bepaald moment in een gebouw bevinden in geval van een noodsituatie.
- **Efficiëntie:** Door de aanwezigheid van mensen in een ruimte te volgen, kunnen beacons worden gebruikt om de bezettingsgraad van een gebouw of kamer te meten. Dit kan helpen bij het plannen van personeel en het toewijzen van middelen, wat de efficiëntie kan verbeteren en de kosten kan verlagen.
- **Analyse:** Door de aanwezigheid van mensen in een ruimte te volgen, kunnen beacons worden gebruikt om het gedrag van mensen te analyseren. Dit kan waardevolle informatie opleveren voor bedrijven en organisaties, zoals hoe lang mensen in een bepaalde ruimte blijven en welke delen van een gebouw het meest worden gebruikt.

In de praktijk kunnen beacons worden gebruikt om gedetailleerde informatie te verkrijgen over de aanwezigheid van mensen in een gebouw, zoals het aantal mensen in specifieke wachtruimtes, gangen of liften. Dit soort gegevens kan bijdragen aan een verbetering van de veiligheid, met name in geval van noodsituaties.

Bovendien kunnen beacons helpen om het bewegingsgedrag van mensen binnen het gebouw in kaart te brengen. Zo kan worden vastgesteld of mensen direct de juiste weg vinden of dat er veel heen en weer wordt gelopen voordat de gewenste bestemming wordt bereikt.

Deze informatie kan ook van nut zijn bij het bepalen van de benodigde verlichting en verwarming in bepaalde gebieden.

Zijn er risico's verbonden aan het volgen van aanwezigheid met beacons?

Zoals bij elk type technologie zijn er ook risico's verbonden aan het volgen van aanwezigheid met beacons. Een van de grootste zorgen is de privacy van gebruikers. Het volgen van aanwezigheid met beacons kan gevoelige informatie over gebruikers onthullen, zoals waar ze zich bevinden en hoe lang ze in een bepaalde ruimte zijn geweest. Het is daarom belangrijk dat bedrijven en organisaties die beacons gebruiken om aanwezigheid te volgen, transparant zijn over hun praktijken en duidelijk communiceren welke gegevens worden verzameld en hoe deze worden gebruikt.

Een ander potentieel risico is beveiliging. Omdat beacons draadloze signalen uitzenden, kunnen ze kwetsbaar zijn voor hacking en andere beveiligingsrisico's. Het is belangrijk dat beacons worden beschermd met sterke beveiligingsmaatregelen, zoals versleuteling van gegevens en beperking van toegang tot de apparaten.

Het volgen van aanwezigheid met beacons kan nuttig zijn voor verschillende toepassingen, waaronder veiligheid, efficiëntie en analyse. Het kan echter ook privacy- en beveiligingsrisico's met zich meebrengen, dus het is belangrijk dat bedrijven en organisaties die beacons gebruiken, verantwoordelijk handelen en de nodige beveiligingsmaatregelen nemen om de gegevens van gebruikers te beschermen. Als deze risico's op een verantwoorde manier worden aangepakt, kunnen beacons een waardevolle toevoeging zijn aan de moderne technologie en de manier waarop we gebouwen en ruimtes beheren en analyseren.

Bonus 1

De inzet van veiligheidscamera's is een wijdverbreide praktijk voor de bescherming van eigendommen en waardevolle zaken.

Echter, recentelijk is een zorgwekkende ontwikkeling aan het licht gekomen. Tijdens een recente cursus werd onthuld dat er in België alleen al meer dan 60 camera's zijn waarvan de beelden vrij toegankelijk zijn op het internet, zonder dat inloggen vereist is.

Deze alarmerende situatie benadrukt de noodzaak van een zorgvuldige selectie en configuratie van beveiligingscamera's.

Hoewel de verleiding groot kan zijn om voor goedkopere opties te gaan, zoals bepaalde camera's van Chinese makelij, is het essentieel om voorzichtig te zijn.

Zelfs bij de aanschaf van camera's van bekende merken, blijft het van cruciaal belang om de instellingen correct te configureren om ongeautoriseerde toegang te voorkomen.

Dit probleem beperkt zich niet tot openbaar toegankelijke live feeds. Het omvat ook systemen die standaard inloggegevens gebruiken, waardoor ze kwetsbaar zijn voor ongeautoriseerde toegang.

Bovendien hebben we ontdekt dat diverse back-upsystemen online beschikbaar zijn, die potentieel openstaan voor 'vrije toegang'.

Dit wijst op een nog grotere kwetsbaarheid en behoefte aan bewustwording.

Ons team is gespecialiseerd in het identificeren van online kwetsbaarheden en kan helpen bepalen welke van uw systemen mogelijk blootgesteld zijn aan hacking risico's.

Hoewel de situatie in Nederland nog alarmerender lijkt, is het essentieel dat mensen zich bewust worden van deze risico's.

Helaas kunnen we geen video maken om deze kwetsbare systemen en hun toegangsmethoden in detail te demonstreren, om juridische en ethische redenen. Het is echter van het grootste belang dat zowel particulieren als bedrijven zich bewust worden van deze kwetsbaarheden en de noodzakelijke stappen ondernemen om hun beveiliging te versterken.

Belangrijke tip

In 2022 werden in de US alleen al 860 grote bedrijven het slachtoffer van Ransomware en waarbij 8% een totaal verlies van gegevens mocht ondervinden.

Dat lijkt niet veel maar deze 860 bedrijven behoren tot de top 1000 grootsten, die eigenlijk hun eigen security diensten hebben.

99,2% lag de oorzaak bij onoplettend personeel die te los en te onvoorzichtig omging met e-mails.

Maar tegenwoordig zijn niet enkel de groten doelwit ook kleinere bedrijven, tot eenmanszaken, apothekers, dokters en zelf prive mensen worden gevisieerd.

We kunnen het maar blijven herhalen, let op, wees aandachtig, denk 2x na en dan nog es extra voor u ergens op klikt of iets openend.

Maak regelmatig backups van uw data.....

Nieuwste ontwikkelingen

Bluetooth Beveiligingslek Ontdekt

Een hacker heeft recent een methode ontdekt om zonder geavanceerde apparatuur toegang te krijgen tot elk nabijgelegen apparaat dat Bluetooth gebruikt, inclusief pc's, Android-telefoons, tablets, Macs en iPhones. Deze kwetsbaarheid treft voornamelijk gebruikers van draadloze toetsenborden. Bij iPhones is het risico beperkt tot die apparaten die ooit verbonden zijn geweest met een Apple Magic Keyboard. Echter, apparaten zoals Macs, MacBook's, Android-apparaten en pc's zijn eveneens gevoelig voor dit lek.

Momenteel is de enige bekende preventieve maatregel het uitschakelen van Bluetooth, wat niet altijd een haalbare oplossing is. De ontdekker van deze kwetsbaarheid, die blijkbaar goede bedoelingen heeft, heeft de betrokken bedrijven geïnformeerd over zijn bevindingen. Hij heeft de methode nog niet gedeeld binnen de hackersgemeenschap. Nu deze informatie echter bekend is, bestaat de kans dat anderen deze kwetsbaarheid zullen proberen te exploiteren.

Eerder was al bekend dat draadloze muizen overgenomen kunnen worden door hackers.

Daarom wordt aanbevolen om, waar mogelijk, bedrade muizen en toetsenborden te gebruiken en onnodige Bluetooth-verbindingen te verwijderen.

We blijven deze ontwikkeling nauwlettend volgen en zullen verdere updates verstrekken zodra er meer informatie beschikbaar komt.

Mousejacking

Het Risico van Draadloze Muizen en Hoe Je Jezelf Kunt Beschermen

Introductie:

In de wereld van technologie en connectiviteit is draadloos gemak een veel gezochte eigenschap. Draadloze muizen hebben de conventionele bekabelde muizen vervangen en bieden gebruikers meer bewegingsvrijheid en flexibiliteit. Echter, zoals bij elk technologisch voordeel, komen er ook risico's om de hoek kijken.

Een van deze risico's is "mousejacking," een potentieel gevaarlijke aanval die kan leiden tot inbreuk op de beveiliging en het lekken van gevoelige informatie.

In dit fragment zullen we dieper ingaan op wat mousejacking is, wat er potentieel kan gebeuren en hoe je jezelf kunt beschermen.

Wat is Mousejacking?

Mousejacking is een beveiligingskwetsbaarheid die voorkomt bij draadloze muizen met een USB-ontvanger. Deze muizen communiceren draadloos met de computer via radiogolven. Helaas zijn sommige van deze draadloze verbindingen onvoldoende beveiligd en kunnen ze kwetsbaar zijn voor aanvallen van buitenaf. Een aanvaller die binnen het bereik van de draadloze ontvanger is, kan de radiogolven onderscheppen en valse commando's naar de computer sturen, zonder dat de gebruiker zich daarvan bewust is.

Potentiële Gevolgen:

Als een aanvaller erin slaagt om een draadloze muis te "jacken", kunnen er verschillende potentiële gevolgen optreden:

1. Ongeautoriseerde toegang:

De aanvaller kan kwaadaardige commando's naar de computer sturen, zoals het uitvoeren van schadelijke software of het openen van een achterdeurtje voor verdere aanvallen. Hierdoor kan de aanvaller ongeautoriseerde toegang krijgen tot gevoelige informatie of het systeem compromitteren.

2. Gegevensdiefstal:

Mousejacking kan leiden tot het stelen van gevoelige informatie, zoals inloggegevens, persoonlijke documenten of bedrijfsgeheimen. De aanvaller kan deze informatie gebruiken voor identiteitsdiefstal, financiële fraude of chantage.

3. Keylogging:

Een aanvaller kan de draadloze verbinding gebruiken om keylogging-functionaliteit te activeren, waardoor elke toetsaanslag die je maakt kan worden vastgelegd. Dit kan leiden tot het verzamelen van wachtwoorden, creditcardgegevens en andere vertrouwelijke informatie.

Hoe te Voorkomen:

Gelukkig zijn er verschillende maatregelen die je kunt nemen om jezelf te beschermen tegen mousejacking:

1. Gebruik een beveiligde draadloze muis:

Kies voor een muis die gebruikmaakt van geavanceerde encryptietechnieken, zoals AES-128 encryptie. Deze muizen bieden een hoger niveau van beveiliging en zijn moeilijker te hacken.

2. Houd software up-to-date:

Zorg ervoor dat je regelmatig de firmware en drivers van je draadloze muis bijwerkt. Fabrikanten brengen vaak beveiligingsupdates uit om bekende kwetsbaarheden aan te pakken.

3. Beperk het bereik:

Mousejacking vereist fysieke nabijheid van de aanvaller. Door het bereik van je draadloze muis te beperken, kun je de kans op een aanval verminderen. Gebruik je muis bijvoorbeeld alleen op korte afstand van je computer.

4. Verwijder ongebruikte draadloze muizen:

Als je oude draadloze muizen hebt die je niet meer gebruikt, verwijder dan de USB-ontvangers of gooi ze veilig weg. Deze ongebruikte muizen kunnen een potentieel beveiligingsrisico vormen.

5. Gebruik een bedrade muis:

Als je je zorgen maakt over de beveiliging, kun je altijd kiezen voor een bedrade muis. Deze muizen zijn niet vatbaar voor mousejacking-aanvallen, omdat ze geen draadloze verbinding hebben.

Mousejacking is een serieus beveiligingsrisico dat draadloze muizen met zich meebrengen. Het kan leiden tot ongeautoriseerde toegang, gegevensdiefstal en andere ernstige gevolgen. Door het volgen van de genoemde preventieve maatregelen kun je jezelf beschermen tegen deze aanvallen. Zorg ervoor dat je altijd bewust bent van de beveiligingsrisico's en neem de nodige stappen om je persoonlijke gegevens en apparaten te beschermen.

Kantnota:

De modernere draadloze muis/klavier zijn tegenwoordig beveiligd echter vele oudere en nog veel in gebruik zijnde draadloze toetsenborden en muis, zijn dat niet. Trouwens de aanvaller moet al redelijk dichtbij zijn om dergelijke aanval te doen < 5 meter. Theoretisch kan het dus, maar in de praktijk niet zo makkelijk. We hebben alles in huis om het te testen maar tot heden geen "oudere muis/klavier gevonden. Wel werkte het met goedkope draadloze muis uit niet nader genoemde winkel.

Onthoud dat draadloos, gelijk staat aan radiogolven en deze kunnen altijd onderschept worden.

Wat is een SIEM?

SIEM staat voor "Security Information and Event Management". Het is een uitgebreid beheersysteem dat organisaties helpt bij het monitoren, detecteren, rapporteren en reageren op beveiligingsincidenten binnen hun IT-omgevingen.

Wat doet een SIEM?

Een SIEM-systeem verzamelt en correleert data van verschillende bronnen binnen een organisatie, zoals firewalls, antivirusprogramma's en intrusion detection systemen. Het doet vervolgens het volgende:

1. Gegevensanalyse:

Het analyseert deze data om normaal gedrag te onderscheiden van verdacht of kwaadaardig gedrag.

2. Alarmen:

Bij detectie van verdachte activiteiten stuurt het systeem real-time waarschuwingen naar beveiligingsteams.

3. Dataopslag:

SIEM-systemen slaan beveiligingslogs op voor toekomstige analyses en naleving van regelgeving.

4. Rapportage:

Het genereert gedetailleerde rapporten over beveiligingsincidenten, trends en kwetsbaarheden.

5. Ondersteuning voor naleving:

Het helpt organisaties te voldoen aan verschillende regelgevingen zoals GDPR, HIPAA en andere.

Waarom is een SIEM nuttig?

1. Real-time beveiligingsmonitoring:

Een SIEM biedt continue monitoring van alle systemen en netwerken, zodat bedreigingen in real-time kunnen worden geïdentificeerd en aangepakt.

2. Geavanceerde dreigingsdetectie:

Met geavanceerde correlatiemogelijkheden kan een SIEM complexe bedreigingspatronen herkennen die anders over het hoofd zouden worden gezien.

3. Naleving van regelgeving:

Veel bedrijven moeten voldoen aan strenge beveiligingsnormen. Een SIEM helpt hierbij door het bewijs te leveren dat nodig is voor audits.

4. Efficiëntie:

Door het automatiseren van de dataverzameling en -analyse kunnen beveiligingsteams zich concentreren op het reageren op echte bedreigingen in plaats van handmatig door logs te moeten ploegen.

Andere nuttige informatie

- Implementatie:

De implementatie van een SIEM kan complex zijn en vereist vaak specialistische kennis. Het is essentieel om te zorgen voor correcte configuratie om valse positieven te minimaliseren en echte bedreigingen effectief te detecteren.

- Kosten:

SIEM-oplossingen kunnen duur zijn, zowel wat betreft aanschaf als beheer. Maar de kosten van een mogelijke data-inbreuk of niet-naleving kunnen nog hoger zijn.

- Continue evolutie:

Met de voortdurende evolutie van cyberdreigingen moet een SIEM-systeem regelmatig worden bijgewerkt en aangepast om effectief te blijven.

Een SIEM is een essentiële tool voor organisaties die hun beveiligingspostuur willen versterken en voldoen aan beveiligingsnormen. Hoewel het implementeren en beheren van een SIEM zijn uitdagingen kan hebben, zijn de voordelen op het gebied van beveiliging, naleving en gemoedsrust aanzienlijk.

Wij kunnen u helpen uw eigen “in-huis” SIEM op te zetten of wij kunnen deze voor beheren.

Belangrijke opmerking

Nu in België Telenet zijn gratis wifi-netwerk stopzet, zullen veel gebruikers met kleinere databundels op zoek gaan naar gratis wifi-hotspots. Het aantal van deze gebruikers is wellicht groter dan Telenet aangeeft.

Wees uiterst voorzichtig bij het verbinden met dergelijke gratis wifi-punten. Hackers kunnen gemakkelijk zo'n hotspot creëren en al uw data volgen en inzien.

Voer nooit betalingen uit of bezoek websites met gevoelige informatie over uzelf of anderen via deze netwerken. Voor dergelijke acties is het raadzaam om uw 3G, 4G of 5G dataverbinding te gebruiken. Als u toch een openbaar wifi-netwerk moet gebruiken, overweeg dan zeker een VPN.

Vermijd gratis VPN-aanbiedingen; kwaliteit heeft vaak zijn prijs. Overweeg een betaalde VPN.

Wij maken zelf gebruik van Surfshark:

<https://surfshark.club/friend/PfxZF2Mh>

Via bovenstaande link kunt u een korting ontvangen, maar uiteraard bent u vrij in uw keuze.

Denk aan uw veiligheid en privacy.

We hebben voor mensen die beroepshalve veel op de baan zijn of op “vreemde” locaties moeten verblijven een Travel Router ontwikkelt met alle mogelijk veiligheid-attributen ingebouwd zodat u ongestoord en met tamelijke zekerheid kunt surfen vanop ongekende wifi netwerken.

Zie verder in het boek hoofdstuk Travel Router

Meer privacy tips

Wil je weten wat google allemaal van u weet? Ga dan naar deze website

<https://myactivity.google.com/>

U kan dit eenvoudig wissen en uitschakelen eventueel (aanrader)

Windows Sandbox

Een veilige speeltuin voor experimenteren en testen.

Inleiding

Windows Sandbox is een handige en innovatieve functie geïntroduceerd door Microsoft in Windows 10 (versie 1903) en later.

Het stelt gebruikers in staat om geïsoleerde, tijdelijke omgevingen te creëren waarin ze applicaties kunnen uitvoeren en experimenteren zonder hun hoofdsysteem in gevaar te brengen.

Met Windows Sandbox kunnen gebruikers potentieel schadelijke of onbekende programma's uitvoeren zonder risico op besmetting van hun werkelijke systeem. In dit artikel zullen we dieper ingaan op wat Windows Sandbox is, hoe het werkt, de voordelen ervan, en hoe het kan worden gebruikt.

Wat is Windows Sandbox?

Windows Sandbox is een gesandboxte omgeving die op een geïsoleerde manier binnen Windows wordt uitgevoerd.

Het is in feite een virtuele machine die wordt geactiveerd wanneer een gebruiker het start en stopt zodra de sessie wordt afgesloten.

Elke keer dat de Sandbox wordt gestart, begint deze met een schone lei, wat betekent dat het geen blijvende wijzigingen in het hoofdsysteem aanbrengt.

Elke toepassing, bestand of wijziging die binnen de Sandbox wordt uitgevoerd, blijft beperkt tot die sessie en heeft geen impact op de rest van het systeem.

Hoe werkt Windows Sandbox?

Windows Sandbox maakt gebruik van de virtualisatietechnologie van Windows om een geïsoleerde omgeving te creëren.

Wanneer je Windows Sandbox start, wordt er een virtuele machine (VM) op de achtergrond gemaakt, waarbinnen een nieuw exemplaar van Windows wordt uitgevoerd.

Deze virtuele machine is echter niet volledig zelfstandig; in plaats daarvan deelt hij bepaalde systeembronnen met het hoofdsysteem, waardoor het lichtgewicht en efficiënt blijft.

Belangrijkste voordelen van Windows Sandbox:

1. Veilige experimenten:

Met Windows Sandbox kunnen gebruikers onbekende of potentieel gevaarlijke toepassingen uitvoeren zonder enig risico voor hun echte systeem.

Het is een uitstekende manier om bestanden te controleren op malware of verdachte software te testen zonder uw pc in gevaar te brengen.

2. Schone lei:

Elke keer dat je de Sandbox start, begin je met een frisse installatie van Windows.

Dit betekent dat eventuele wijzigingen die je aanbrengt in de Sandbox, zoals downloads of tijdelijke bestanden, automatisch worden verwijderd zodra je de sessie afsluit.

3. Geen impact op prestaties:

Aangezien de Sandbox als een lichte VM wordt uitgevoerd en alleen actief is wanneer je het gebruikt, heeft het geen blijvende invloed op de prestaties van je hoofdsysteem.

4. Geen configuratie nodig:

Windows Sandbox wordt standaard meegeleverd met Windows 10 Pro- en Enterprise-edities (versie 1903 en hoger). Er is geen behoefte aan extra installaties, configuraties of licenties.

Hoe Windows Sandbox te gebruiken:

1. Controleer de vereisten:

Zorg ervoor dat je de Windows 10 Pro- of Enterprise-editie (versie 1903 of later) gebruikt, omdat Windows Sandbox niet beschikbaar is in Windows 10 Home. Ook moet de hardware virtualisatie zijn ingeschakeld in het BIOS.

2. Activeer Windows Sandbox:

Zoek in het startmenu naar "Windows Sandbox" en start het programma. De Sandbox-omgeving wordt gestart in een nieuw venster.

3. Voer je experimenten uit:

Binnen de Sandbox kun je toepassingen installeren, bestanden downloaden, testen en experimenteren zoals je normaal zou doen, maar zonder gevolgen voor je hoofdsysteem.

4. Sluit de Sandbox af:

Zodra je klaar bent met je sessie, sluit je de Sandbox af. Alle wijzigingen die je hebt aangebracht, worden automatisch verwijderd, en de volgende keer dat je Sandbox start, begin je weer met een schone lei.

Windows Sandbox is een krachtige functie die een veilige omgeving biedt voor gebruikers om te experimenteren, testen en potentieel gevaarlijke toepassingen uit te voeren zonder hun hoofdsysteem in gevaar te brengen.

Met zijn lichte en efficiënte aanpak is het een geweldig hulpmiddel voor iedereen die graag software en bestanden wil testen zonder angst voor schadelijke gevolgen.

Als je Windows 10 Pro of Enterprise of latere versies gebruikt, is het zeker de moeite waard om Windows Sandbox te proberen en je computerervaring naar een hoger niveau te tillen.

Data Verbergen

Het Geheimzinnige Pad van Digitale Verborgene Schatten
Introductie:

In de huidige digitale wereld, waar privacy en veiligheid steeds belangrijker worden, zoeken mensen vaak naar manieren om gevoelige informatie te beschermen.

Eén techniek die populair is geworden, is het verbergen van data in ogenschijnlijk onschuldige bestanden, zoals foto's of andere documenten.

In dit hoofdstuk zullen we ontdekken wat het verbergen van data inhoudt, waarom het kan worden gebruikt, de wettelijke aspecten ervan, de mogelijke gevaren en hoe je verborgen data kunt ontdekken.

Wat is het verbergen van data?

Het verbergen van data, ook bekend als steganografie, is het proces waarbij geheime informatie wordt ingebed in onopvallende bestanden zonder dat het voor anderen detecteerbaar is.

Dit kan worden gedaan door de bits van de verborgen data in de structuur van het bestand te verweven, zoals de kleurinformatie van een afbeelding, de audiogegevens van een liedje, of zelfs de tekst van een document.

Waarom wordt het gebruikt?

Het verbergen van data kan verschillende doeleinden hebben, waaronder:

1. Vertrouwelijkheid:

Het biedt een middel om gevoelige informatie te beschermen tegen ongeautoriseerde toegang. Door gegevens te verbergen in ogenschijnlijk onschuldige bestanden, kunnen gebruikers communiceren zonder dat anderen vermoeden dat er iets geheims gaande is.

2. Steganografische kunst:

Voor sommige mensen is het verbergen van data een vorm van creatieve expressie. Ze genieten van het ontwerpen van verborgen boodschappen of kunstwerken binnen bestanden, waarbij de uitdaging ligt in het creëren van iets dat zowel onzichtbaar als betekenisvol is.

Is het legaal?

De wettelijke aspecten van het verbergen van data kunnen variëren afhankelijk van het gebruik en de intentie ervan.

In veel rechtsgebieden is het verbergen van persoonlijke of vertrouwelijke informatie voor legitieme doeleinden wettelijk toegestaan. Echter, het gebruik van steganografie met het oog op criminele activiteiten, zoals het verbergen van malware of illegale inhoud, is uiteraard illegaal en strafbaar.

Potentiële gevaren van het verbergen van data:

Hoewel het verbergen van data nuttig kan zijn, zijn er enkele potentiële gevaren om rekening mee te houden:

1. Misbruik van informatie:

Als gevoelige informatie op onbedoelde wijze in verkeerde handen valt, kan dit leiden tot identiteitsdiefstal, chantage of andere vormen van misbruik.

2. Onbedoelde verspreiding:

Bij het delen van bestanden waarin verborgen data aanwezig is, bestaat het risico dat anderen de verborgen informatie onbedoeld ontdekken en verspreiden, zonder zich bewust te zijn van de potentiële consequenties.

Hoe verborgen data te ontdekken:

Het ontdekken van verborgen data kan een uitdaging zijn, omdat het doelbewust ontworpen is om onzichtbaar te zijn. Sommige methoden om verborgen data te ontdekken zijn:

1. Stenografie-tools:

Er zijn speciale softwaretools beschikbaar die kunnen helpen bij het detecteren van verborgen data in bestanden. Deze tools kunnen patronen, afwijkingen of verborgen informatie aan het licht brengen.

2. Analyse van bestandsstructuur:

Het bestuderen van de interne structuur van een bestand kan soms aanwijzingen onthullen die wijzen op de aanwezigheid van verborgen data. Dit vereist echter technische kennis en begrip van bestandsformaten.

Het verbergen van data is een fascinerende techniek die mensen in staat stelt geheime informatie te beschermen of steganografische kunstwerken te creëren. Hoewel het legaal en nuttig kan zijn in bepaalde contexten, brengt het verbergen van data ook potentiële gevaren met zich mee, zoals misbruik van informatie. Het ontdekken van verborgen data kan een uitdaging zijn en vereist vaak gespecialiseerde tools of technische kennis.

Wees altijd bewust van de wettelijke aspecten en ethische overwegingen bij het gebruik van het verbergen van data en houd rekening met de mogelijke gevolgen van het delen van bestanden met verborgen informatie.

Hoe mogelijks snel te herkennen?

Indien het desbetreffende bestand zoals foto, document of andere veel te groot lijkt te zijn in vergelijking met een ander gelijkaardig document.

Het belang van onze digitale voetafdruk

Begrijpen, beheren en beschermen

In de moderne samenleving is de digitale wereld een integraal onderdeel geworden van ons dagelijks leven.

Elke keer dat we online surfen, berichten versturen of sociale media gebruiken, laten we digitale sporen achter die onze digitale voetafdruk vormen.

Onze digitale voetafdruk is een verzameling van onze online activiteiten en het digitale spoor dat we achterlaten op verschillende platforms en apparaten.

In deze blogpost zullen we verkennen wat een digitale voetafdruk is, wat het doet, wie het gebruikt en waarom het belangrijk is om deze te beheren en te beschermen. We zullen ook ingaan op de mogelijke gevaren en wat we kunnen doen om onze digitale voetafdruk te beschermen.

Wat is een digitale voetafdruk?

Een digitale voetafdruk is het spoor van informatie dat we achterlaten wanneer we online actief zijn.

Het omvat persoonlijke gegevens, zoals onze naam, leeftijd, adres en e-mailadres, maar ook onze online gewoonten, interesses, aankopen en interacties met andere mensen en platforms. Deze informatie kan worden verzameld en geanalyseerd door verschillende partijen, zoals sociale mediabedrijven, adverteerders, zoekmachines en overheidsinstanties.

Wat doet een digitale voetafdruk?

Onze digitale voetafdruk heeft verschillende doeleinden.

Ten eerste wordt het gebruikt voor gerichte reclame. Adverteerders volgen onze online activiteiten om advertenties op maat te maken op basis van onze interesses en voorkeuren.

Ten tweede wordt het gebruikt voor marktonderzoek en het verbeteren van producten en diensten. Bedrijven analyseren de digitale voetafdruk van gebruikers om inzicht te krijgen in consumentengedrag en om trends te identificeren.

Ten derde wordt het gebruikt voor veiligheids- en beveiligingsdoeleinden. Overheden en instanties kunnen digitale voetafdrukken volgen om potentiële bedreigingen te detecteren en criminele activiteiten op te sporen.

Wie gebruikt onze digitale voetafdruk en waarom?

Verschillende partijen maken gebruik van onze digitale voetafdruk.

Sociale mediabedrijven en online platforms verzamelen en analyseren deze gegevens om advertenties te personaliseren en gebruikerservaringen te verbeteren.

Adverteerders gebruiken onze digitale voetafdruk om gerichte advertenties te tonen, wat hen helpt om hun producten en diensten effectiever te promoten.

Overheden en wetshandhavingsinstanties kunnen digitale voetafdrukken volgen om veiligheidsredenen en om criminaliteit te bestrijden.

Hoe gevaarlijk kan een digitale voetafdruk zijn?

Hoewel een digitale voetafdruk voordelen kan bieden, zijn er ook potentiële gevaren verbonden aan het verzamelen en gebruiken van deze informatie.

Ten eerste kan het leiden tot inbreuk op de privacy. Wanneer persoonlijke gegevens onbedoeld in verkeerde handen vallen of worden misbruikt, kan dit leiden tot identiteitsdiefstal, oplichting of reputatieschade.

Ten tweede kan het leiden tot manipulatie en beïnvloeding. Door onze digitale voetafdruk te analyseren, kunnen bedrijven en organisaties gerichte inhoud creëren om ons gedrag, onze beslissingen en zelfs onze politieke opvattingen te beïnvloeden.

Hoe kunnen we onze digitale voetafdruk beschermen?

Het beschermen van onze digitale voetafdruk is van cruciaal belang.

Hier zijn enkele belangrijke stappen die we kunnen nemen:

1. Gegevensbewustzijn:

Wees bewust van welke persoonlijke gegevens je deelt en met wie. Lees privacy beleid en overweeg het beperken van de informatie die je deelt.

2. Sterke wachtwoorden en beveiligingsmaatregelen:

Gebruik unieke, sterke wachtwoorden voor elk online account en schakel tweefactorauthenticatie in waar mogelijk.

3. Privacy-instellingen:

Controleer en pas de privacy-instellingen aan op sociale media en andere online platforms. Beperk de zichtbaarheid van je persoonlijke informatie.

4. Cookies en tracking:

Beheer je cookies en trackingvoorkeuren in je webbrowswer. Overweeg het blokkeren van ongewenste trackers en gebruik browserextensies die je privacy beschermen.

5. Beperk openbare Wi-Fi:

Vermijd het gebruik van openbare Wi-Fi-netwerken voor het delen van gevoelige informatie. Gebruik indien mogelijk een VPN (Virtual Private Network) voor een veiligere internetverbinding.

6. Bewustzijn van phishing:

Wees voorzichtig met e-mails en berichten van onbekende afzenders. Wees op je hoede voor phishing-pogingen en klik niet op verdachte links.

7. Periodieke gegevensopruiming:

Verwijder regelmatig oude accounts, onnodige apps en ongebruikte gegevens om de hoeveelheid persoonlijke informatie te minimaliseren.

Door bewust te zijn van onze digitale voetafdruk en proactieve maatregelen te nemen om deze te beschermen, kunnen we de risico's verminderen en controle houden over onze privacy en online veiligheid.

Onze digitale voetafdruk kan ons helpen om naadloos door de digitale wereld te navigeren, maar het is belangrijk om te onthouden dat we de eigenaren zijn van onze gegevens.

Door bewustzijn, voorzichtigheid en proactieve stappen te nemen, kunnen we onze digitale voetafdruk beheren en beschermen, waardoor we veiliger en meer controle hebben over ons online bestaan.

Metadata

De sleutel tot informatiebeheer en privacy

Introductie:

In onze moderne wereld, waar digitale gegevens een integraal onderdeel van ons leven zijn geworden, speelt metadata een cruciale rol. Hoewel het vaak over het hoofd wordt gezien, is metadata een krachtig hulpmiddel dat wordt gebruikt om informatie te beheren, te categoriseren en te analyseren.

Het begrijpen van wat metadata is, wat het doet, wie het gebruikt en hoe ermee om te gaan, is van essentieel belang om onze privacy te beschermen en de controle over onze gegevens te behouden.

Wat is metadata?

Metadata kan worden beschouwd als "gegevens over gegevens". Het zijn contextuele informatie-elementen die beschrijvende kenmerken van gegevenssets bevatten.

Het gaat niet zozeer om de inhoud van de gegevens zelf, maar om informatie zoals de datum van creatie, de auteur, de bestandsgrootte, de locatie en de structuur van de gegevens. Metadata fungeert als een soort "etiket" dat helpt bij het organiseren, doorzoeken en begrijpen van gegevens.

Wat doet metadata?

Metadata biedt belangrijke informatie over gegevens en stelt ons in staat deze efficiënter te beheren en te analyseren.

Het vergemakkelijkt het proces van gegevensontdekking en -toegang door zoekmachines en gegevensbanken te helpen relevante resultaten te produceren.

Metadata kan ook worden gebruikt om de betrouwbaarheid en kwaliteit van gegevens te evalueren, aangezien het inzicht geeft in de herkomst en de bewerkingsgeschiedenis van de gegevens.

Wie gebruikt metadata en waarom?

Metadata wordt gebruikt door verschillende belanghebbenden, waaronder:

1. Gegevensbeheerders: Metadata stelt beheerders in staat om gegevens efficiënter te organiseren, bij te werken en te archiveren. Het verbetert de zoekfunctionaliteit en helpt bij het identificeren van relevante gegevensbronnen.

2. Onderzoekers en wetenschappers: Metadata speelt een essentiële rol bij het delen en verifiëren van onderzoeksgegevens. Het vergemakkelijkt de replicatie van studies en draagt bij aan de transparantie en reproduceerbaarheid van wetenschappelijk werk.

3. Bedrijven en marketeers: Metadata wordt gebruikt om klantgedrag en voorkeuren te analyseren, waardoor bedrijven hun marketingstrategieën kunnen afstemmen op specifieke doelgroepen. Het helpt ook bij het beheer van digitale bedrijfsmiddelen en het waarborgen van naleving van regelgeving.

4. Overheidsinstanties en wetshandhavers: Metadata kan worden gebruikt voor het traceren van communicatie en het uitvoeren van onderzoeken. Het kan waardevol bewijsmateriaal opleveren bij het bestrijden van criminaliteit en terrorisme.

Wat kun je doen om je privacy te beschermen tegen metadata?

1. Gegevensminimalisatie: Beperk de hoeveelheid persoonlijke informatie die je deelt en vermijd het verstrekken van onnodige metadata.

2. Encryptie: Maak gebruik van end-to-end encryptie voor communicatie om ervoor te zorgen dat je gegevens niet zonder jouw toestemming kunnen worden gelezen.

3. Anonimisering: Overweeg het anonimiseren van gegevens voordat je ze deelt, zodat persoonlijke identificeerbare informatie wordt verwijderd of vervangen door fictieve gegevens.

4. Bewustwording: Wees je bewust van de gegevens die je online deelt en begrijp hoe metadata kan worden gebruikt om je te volgen of te profileren.

Metadata is een krachtig instrument dat wordt gebruikt om gegevens te beheren en te analyseren. Hoewel het waardevol is voor verschillende belanghebbenden, is het ook belangrijk om bewust te zijn van de mogelijke gevolgen voor privacy. Door bewuste keuzes te maken over het delen van gegevens en gebruik te maken van beschermende maatregelen zoals encryptie en anonimisering, kunnen we onze privacy beschermen en controle houden over onze gegevens in dit digitale tijdperk.

Waarom metadata ook gevaarlijk kan zijn:

1. Profilering en surveillance:

Metadata kan worden gebruikt om gedragspatronen, interesses en voorkeuren van individuen te analyseren. Door het verzamelen en analyseren van metadata kunnen organisaties en overheden gedetailleerde profielen van mensen maken, wat leidt tot surveillance en mogelijk misbruik van persoonlijke informatie.

2. Privacy schending:

Hoewel metadata op zichzelf geen directe persoonlijke informatie bevat, kan het worden gekoppeld aan andere gegevensbronnen om een gedetailleerd beeld van een persoon te vormen. Dit kan leiden tot privacy schendingen wanneer individuen worden blootgesteld aan ongewenste advertenties, doelgerichte marketing of zelfs identiteitsdiefstal.

3. Geolocatie:

Metadata zoals GPS-coördinaten kunnen onthullen waar een foto is genomen of waar een persoon zich op een bepaald moment bevindt. Als deze gegevens in verkeerde handen vallen, kunnen ze worden misbruikt voor stalking, inbraak of andere criminele activiteiten.

4. Informatielekken:

Metadata kan per ongeluk gevoelige informatie bevatten die niet bedoeld was om te worden gedeeld. Bij het delen van documenten of afbeeldingen kunnen onopgemerkte metadata zoals auteursnamen, revisiegeschiedenis of onzichtbare tekst aanwezig zijn, wat kan leiden tot onbedoelde informatie-onthullingen.

5. Data-analyse en profiling:

Organisaties kunnen metadata gebruiken om uitgebreide analyses uit te voeren en gedetailleerde profielen van individuen te creëren. Deze profielen kunnen worden gebruikt voor gerichte reclame, manipulatie van consumentengedrag en besluitvorming zonder dat mensen zich daarvan bewust zijn.

Het is belangrijk om te erkennen dat metadata, ondanks de voordelen die het biedt, ook risico's met zich meebrengt. Het bewustzijn van deze risico's en het nemen van proactieve maatregelen om onze privacy te beschermen, zijn essentieel in een wereld waar gegevens een steeds waardevoller bezit worden.

De kampioenen in het verzamelen van metadata omtrent een persoon zijn bvb Facebook, Google, TikTok, Snapchat en andere social media platformen.

De algoritmes gebruikt door Facebook op basis van uw metadata bvb zorgt ervoor dat u “geschikte advertenties” ziet, linken legt maar mogelijke mensen die u “misschien kent” en zoveel meer.

USB-Datablockers

Bescherming tegen gegevensdiefstal via kwaadaardige USB-apparaten

Introductie:

In de moderne digitale wereld zijn we voortdurend bezig met het beschermen van onze gegevens tegen verschillende vormen van bedreigingen.

Een van de minder bekende maar gevaarlijke risico's is gegevensdiefstal via "bad USB"-apparaten. Gelukkig bieden USB-datablockers een effectieve bescherming tegen dit soort aanvallen.

We leggen kort uit wat een USB-datablocker is, hoe het werkt en waarom het essentieel is om jezelf te beschermen tegen kwaadwillende USB-apparaten.

Wat is een USB-datablocker?

Een USB-datablocker is een speciale hardware tool die de toegang tot jouw USB-poorten beveiligt en voorkomt dat kwaadwillende USB-apparaten jouw gegevens kunnen stelen of malware kunnen injecteren. Het is ontworpen om te voorkomen dat een "bad USB" toegang krijgt tot jouw systeem en schadelijke acties kan uitvoeren.

Hoe werkt een USB-datablocker?

Een USB-datablocker werkt door de communicatie tussen de USB-poort van jouw apparaat en een extern USB-apparaat (lees oplaadkabel/ oplaad adapter) te controleren en te beperken. Het kan bijvoorbeeld de stroomtoevoer naar een USB-poort beperken, waardoor het onmogelijk wordt om gegevens over te dragen.

Waarom is een USB-datablocker essentieel?

1. Bescherming tegen gegevensdiefstal:

Kwaadwillende personen kunnen geïnfecteerde USB-sticks of andere USB-apparaten (lees oplaadkabel /oplaadadapter) gebruiken om ongemerkt toegang te krijgen tot jouw systeem en gegevens te stelen. Met een USB-datablocker kun je voorkomen dat dergelijke apparaten toegang krijgen tot jouw USB-poorten, waardoor jouw gegevens veilig blijven.

2. Voorkomen van malware-infecties:

“Bad USB”-apparaten kunnen ook schadelijke software of malware op jouw systeem injecteren, wat kan leiden tot ernstige beveiligingsrisico's en gegevensverlies. Door gebruik te maken van een USB-datablocker kun je de kans op dergelijke infecties aanzienlijk verminderen, aangezien de toegang tot jouw USB-poorten wordt beperkt.

3. Bescherming van bedrijfsnetwerken:

Voor bedrijven is de bescherming tegen gegevensdiefstal en malware-infecties van cruciaal belang. USB-datablockers spelen een essentiële rol bij het handhaven van de beveiliging van bedrijfsnetwerken. Door het gebruik van USB-datablockers kunnen organisaties voorkomen dat onbevoegde USB-apparaten toegang krijgen tot bedrijfssystemen, waardoor gevoelige bedrijfsgegevens beschermd blijven en het risico op datalekken wordt verminderd.

4. Bescherming van persoonlijke privacy:

Niet alleen bedrijven, maar ook individuele gebruikers kunnen profiteren van USB-datablockers om hun persoonlijke gegevens te beschermen. Of je nu jouw laptop gebruikt in openbare ruimtes, zoals luchthavens of cafés, of jouw computer deelt met anderen, een USB-datablocker zorgt ervoor dat jouw gegevens veilig blijven en niet kunnen worden gestolen via kwaadwillende USB-apparaten.

Met de toenemende dreiging van gegevensdiefstal en malware-infecties via kwaadwillende USB-apparaten, is het essentieel om jouw systemen te beschermen met een USB-datablocker.

Deze tool bieden een effectieve manier om de toegang tot USB-poorten te controleren en te beperken, waardoor gegevensdiefstal en malware-infecties worden voorkomen.

Of je nu een individuele gebruiker bent die jouw persoonlijke privacy wilt beschermen of een bedrijfseigenaar die de beveiliging van bedrijfsgegevens waarborgt, een USB-datablocker is een waardevol hulpmiddel dat bijdraagt aan een veiliger digitale omgeving.

Investeer in een betrouwbare USB-datablocker om jouw gegevens te beschermen tegen de dreiging van kwaadwillende USB-apparaten.

Dergelijke “bad usb” toestellen kunnen eruit zien als een doodgewone usb stick, oplaadkabel, oplaad adapter, eigenlijk kunnen ingebouw worden in ieder usb toestel.

Daarom wees extreem voorzichtig en vermijd de overal vrij beschikbare oplaadpunten in publieke plaatsen, gebruik steeds uw eigen kabel en adapter, indien u niet beschikt over een datablocker.

Deze zijn bij ons verkrijgbaar.

Maak niet de fout door te denken dat alle oplaadkabels dezelfde zijn!

Op vakantie? Denk even na

Met de vakantieperiode in het vooruitzicht, waarin zowel scholen als bouwbedrijven hun verlofperiode ingaan, trekken velen erop uit naar verschillende vakantiebestemmingen.

Terwijl de voorbereidingen tot in de puntjes zijn geregeld, inclusief bagage, reisdocumenten en uitstapjes, wordt vaak de digitale veiligheid vergeten.

Het blijft echter essentieel om in contact te blijven met het thuisfront, via sociale media, maar mogelijk ook voor bankzaken en andere communicatie met gevoelige informatie.

Niet iedereen beschikt over grote databundels voor 3G/4G/5G, omdat er overal wel wifi is, zelfs gratis. Maar is dat echt zo veilig als u denkt?

Het korte antwoord is nee.

Hackers weten dat de drukke vakantieperiode eraan komt en maken daar graag gebruik van.

Om het simpel te houden: gebruik **NOOIT** openbare en/of gratis wifi-netwerken op openbare plaatsen, vooral niet voor bankzaken of het inloggen op locaties waar gevoelige informatie te vinden is. Even snel surfen naar een website is nog enigszins acceptabel, maar voor alles wat enigszins gevoelig is, dient u uw mobiele data te gebruiken.

Mocht er echt geen andere optie zijn, maak dan zeker gebruik van een betalende VPN-service, aangezien gratis VPN's helaas niet voldoende veiligheid kunnen bieden.

En hoe zit het met wifi op campings of in hotels? Ook dan is het beter om een VPN te gebruiken.

Oh nee, uw batterij is leeg! Snel een oplaadpunt zoeken, is dat veilig?
Nee!

Gebruik alsjeblieft altijd je eigen oplader en oplaadkabel of maak gebruik van een datablokker (verkrijgbaar bij ons).

Hackers kunnen namelijk toegang krijgen tot je gegevens via de oplaadpoort.

Dit is de realiteit!

Om echt veilig te zijn, is het raadzaam om wifi en bluetooth uit te schakelen op drukke openbare plaatsen, zoals luchthavens en treinstations.

En is het veilig om blindelings een QR-code te scannen?
Nee!

Wij willen ervoor zorgen dat uw vakantie niet alleen ontspannend is, maar ook veilig wat betreft uw digitale activiteiten. Neem de nodige voorzorgsmaatregelen en blijf op de hoogte van de laatste tips en adviezen om uw digitale veiligheid te waarborgen.

Neem contact met ons op voor meer informatie, zorg ervoor dat u goed voorbereid bent op uw vakantieavonturen.

U ben minder veilig dan u denkt!

Wat ons aan de man gebracht wordt, als gebruikers gemak, veiligheid en zo verdere is in veel gevallen een veel grotere bedreiging dan bvb de eindeloze discussie over de klimaatverandering, het milieu, het elektrisch rijden en noem maar op.

De huidige en zeker de aankomende digitale wereld, digitale munt en de nieuwe technologieën zijn veel meer en een dichtere bedreiging dan u vermoed, en waar mensen niet bij stilstaan. Paranoïde moet het nu ook niet zijn, maar veel meer aandacht aan uw digitale omgeving kan al heel veel helpen.

Uw elektrische poort veilig en wel dicht?

Nee een kwaadwillend individu kopieert uw radiosignaal van uw garagebakje met dezelfde snelheid van uw druk op het knopje.

Uw badge op de werkvloer 3 seconden achterlaten kan fatale gevolgen hebben.

Eén klik op de verkeerde link en foetsie is uw data (lees foto's, brieven, facturen, dossiers)

Stel een kwaadwillende kopieert het radiosignaal van uw garage poort. Op een nacht opent hij uw garage (geen inbraaksporen) haalt uw garage leeg en sluit deze weer mooi. S 'morgens gaat u naar uw garage en weg is alles! Hoe gaat u dat uitleggen aan politie en verzekering?

Of het computer systeem registreert toegang tot uw kantoor van medewerker xyz, terwijl deze eigenlijk rustig thuis tv zit te kijken?

U hebt een alarmsysteem en camera's maar op het ogenblik van een fysieke inbraak blijkt geen alarm af te gaan, geen beelden op de camera want u wifi ligt net op dat moment "plat"

We kunnen zo nog even doorgaan, maar ik vermoed dat u al heel goed beseft waar ik naartoe ga. Dit zijn zaken die u persoonlijk treffen en die vermeden konden worden eventueel.

A.i. en hacking

We kunnen er niet meer omheen A.I. Is er en zal blijven en alleen maar krachtiger en beter worden.

Deep Fake = gezicht wisselen mooiste voorbeeld was te zien bij AGT met het gezicht van Elvis. Daar goed bedoeld maar de “bad guys” zagen andere mogelijkheden.

Nu is er ook Voice Fake, en met een fragment van 3 tot 5 seconden kan de computer uw stem nabootsen en bijgevolg uw nep stem alles laten vertellen wat de “bad boys” dat u wilt horen.

Krijg je dus een telefoontje van moeder, vader, dochter, zoon of vrienden of kennissen, en die vragen om geld dan is het beste wat u kan doen

1. Opleggen en hun nummer terugbellen
2. Spreek op voorhand een soort code woord of zin af, in vraag vorm, stel die vraag, krijg je juiste antwoord ok dan, krijg je ander antwoord let dan heel goed op.

Zo kun je vraag bvb stellen hoe laat kom je thuis? Als het afgesproken antwoord (tijdstip eventueel of ander antwoord) niet overeenkomt met jullie afgesproken antwoord dan is er wat mis.

Krijg je telefoon van onbekend nummer vermijd het woord “ ja “ te zeggen, herhaal als men dit vraagt ook niet uw volledige naam of geboortedatum.

Antwoord liever volledig neutraal

Stof voor een volgend boek

Achtergrondinformatie over Wi-Fi Protected Setup of WPS

Wi-Fi Protected Setup (WPS) is een methode om eenvoudig draadloze netwerken op te zetten. Het doel van WPS is om het gemakkelijker te maken voor niet-technische gebruikers om hun draadloze access points te configureren en apparaten aan te sluiten op het netwerk.

In plaats van het handmatig invoeren van netwerkgegevens, kunnen gebruikers eenvoudigweg de WPS-knop op hun router indrukken en vervolgens de WPS-knop op hun apparaat. Dit zorgt ervoor dat de apparaten automatisch verbinding maken met het netwerk, zonder de noodzaak van het invoeren van een wachtwoord.

Een van de manieren waarop WPS werkt, is door het gebruik van een 8-cijferige pincode. Deze pincode wordt vaak afgedrukt op de router zelf of op een label dat aan de router is bevestigd. Het idee is dat een apparaat, zoals een smartphone of een laptop, kan worden geauthentiseerd met deze pincode en vervolgens automatisch verbinding kan maken met het draadloze netwerk.

Een probleem met WPS is echter dat deze methode kwetsbaar is voor aanvallen. Als een kwaadwillende persoon toegang heeft tot de pincode, kunnen ze deze gebruiken om toegang te krijgen tot het draadloze netwerk. Een veelgebruikte aanvalsmethode is het kraken van de WPS-pincode door middel van brute force. Dit houdt in dat de aanvaller alle mogelijke combinaties van de 8-cijferige pincode probeert totdat de juiste is gevonden.

Gelukkig hebben de fabrikanten van routers een control getal toegevoegd aan de 8-cijferige pincode om deze aanvalsmethode moeilijker te maken. Het controle getal is het achtste cijfer van de pincode en wordt berekend op basis van de eerste zeven cijfers. Hierdoor wordt het aantal mogelijke combinaties verkleind tot ongeveer 10 miljoen.

Sommige fabrikanten hebben de 8-cijferige pincode opgesplitst in twee delen: de eerste vier cijfers en de laatste drie cijfers. Dit betekent dat de aanvaller eerst de eerste vier cijfers moet kraken, wat slechts 10.000 mogelijkheden oplevert, en vervolgens de laatste drie cijfers, wat slechts 1000 mogelijkheden oplevert. In totaal zijn er dus slechts 11.000 mogelijkheden om de WPS-pincode te kraken.

Hoewel WPS bedoeld is om het configureren van draadloze netwerken gemakkelijker te maken, kan het gebruik ervan ook leiden tot beveiligingsproblemen. Het is daarom belangrijk om de beveiligingsinstellingen van de router zorgvuldig te configureren en het gebruik van WPS te beperken als dit niet nodig is.

Eenmaal de hacker uw WPS code kent, mag u nog zoveel van wachtwoord veranderen als u wilt hij zal steeds toegang hebben tot uw wifi netwerk.

Gouden tip:

Zet daar waar mogelijk de WPS functie af in uw router

Het Dubbele Snijvlak van URL Shorteners: Gemak versus Risico

Je komt ze overal tegen de link verkorters - url shortners zoals bitly enzo. Maar er schuilt daar een groot gevaar achter want je weet eigenlijk niet waarheen die link gaat als je erop klikt. En daar maken veel hacker gretig gebruik van.

Via deze website kan je eerst kijken na ingeven van de short link, waar deze effectief naartoe gaat.

Wees voorzichtig, wees aandachtig, en denk voor je op zo'n verkorte link klikt

<https://checkshorturl.com/>

In het digitale tijdperk, waar snelheid en efficiëntie hoog in het vaandel staan, hebben URL-verkorters (URL shorteners) zich opgeworpen als onmisbare hulpmiddelen. Ze transformeren lange, onhandige webadressen in korte, deelbare links die gemakkelijk te onthouden en te verspreiden zijn.

Diensten als Bit.ly en TinyURL hebben de manier waarop we links delen op sociale media, in e-mails en andere digitale communicatievormen, revolutionair veranderd. Ondanks hun onmiskenbare gebruiksgemak, schuilen er echter significante veiligheidsrisico's in het gebruik van URL-verkorters. Deze risico's vereisen een grondig begrip en voorzichtige benadering.

Waarom worden URL-verkorters gebruikt?

Compactheid:

Ze verminderen de lengte van URL's, wat essentieel is voor platforms met karakterlimieten, zoals Twitter.

Esthetiek:

Korte links ogen netter en zijn minder overweldigend voor de ontvanger.

Tracking:

Velen bieden geavanceerde analytics, waardoor contentmakers en marketeers het klikgedrag kunnen volgen.

Beheersbaarheid:

Ze maken het mogelijk om links na publicatie te wijzigen zonder de oorspronkelijke URL te veranderen.

Potentiële Gevaren

Ondanks deze voordelen brengen URL-verkorters aanzienlijke risico's met zich mee:

Verhuld Bestemming: Korte links maskeren de eindbestemming, waardoor ze een perfect middel zijn voor cybercriminelen om gebruikers naar kwaadaardige websites te leiden.

Phishing en Malware:

Ze worden vaak gebruikt in phishing-aanvallen en om malware te verspreiden, aangezien de werkelijke URL niet zichtbaar is.

Vertrouwenskwesties:

Gebruikers kunnen aarzelen om op verkorte links te klikken omdat ze zich bewust zijn van de mogelijke risico's.

Dienst Afhankelijkheid:

Als de verkortingsdienst offline gaat, werken alle gecreëerde links niet meer, wat kan leiden tot gebroken links op het web.

Veiligheidsmaatregelen

Om je te beschermen tegen de schaduwzijde van URL-verkorters, kun je de volgende veiligheidsmaatregelen toepassen:

Gebruik Betrouwbare Diensten:

Kies voor verkortingsdiensten met een goede reputatie en veiligheidsmaatregelen.

Preview Functies:

Sommige verkorters bieden een preview-functie. Door bijvoorbeeld "preview" voor de link te plaatsen, kun je de bestemming zien zonder er direct heen te gaan.

Beveiligingstools:

Installeer browserextensies of gebruik online tools die verkorte links scannen voordat je ze bezoekt.

Wees Voorzichtig:

Als een link verdacht lijkt, bijvoorbeeld door de context waarin hij is ontvangen, klik er dan niet op.

Educatie:

Bewustwording creëren over de risico's van verkorte links is essentieel. Informeer jezelf en anderen over hoe je veilig kunt blijven.

URL-verkorters zijn zowel een zegen als een vloek. Ze bieden ongeëvenaard gemak in onze digitale communicatie, maar openen tegelijkertijd deuren voor misbruik door cybercriminelen.

Door de juiste voorzorgsmaatregelen te treffen en een bewuste gebruiker te zijn, kun je de voordelen van URL-verkorters benutten terwijl je de risico's minimaliseert. In de strijd tegen cyberdreigingen is kennis je beste verdediging. Sta dus altijd kritisch tegenover de links die je aanklikt en deel, zeker als ze verkort zijn.

De Travel Router

Met de vakantieperiode in aantocht kijken velen van ons uit naar een welverdiende pauze. Tijdens onze reizen willen we graag verbonden blijven met het thuisfront, onze sociale media volgen, en meer. Vaak bieden hotels en andere verblijfplaatsen gratis wifi aan, terwijl sommigen hier een vergoeding voor vragen. Dit kan betekenen dat voor een gezin van vier, elk lid afzonderlijk moet betalen voor toegang, wat aanzienlijk in de kosten kan lopen. Bovendien rijst de vraag hoe veilig deze netwerken zijn. Wie kan er mogelijk meekijken met wat u online doet? Zijn er restricties op wat u kunt bekijken, of beperkt het land bepaalde websites? En is het veilig om te bankieren over deze wifi?

Gelukkig bestaat er een oplossing die niet alleen kostenefficiënt is, maar ook uw privacy en veiligheid waarborgt. We bieden geen standaardproduct, maar een op maat gemaakte oplossing: de reisrouter. Deze slimme tool stelt u in staat om met het hele gezin gebruik te maken van één enkele wifi-aansluiting, terwijl alle data en verbindingen veilig verlopen via een Virtual Private Network (VPN). Dit betekent dat u niet alleen bespaart op de kosten van meerdere aansluitingen, maar ook gegarandeerd bent van een veilige en privé internetverbinding, ongeacht waar u bent.

Met onze reisrouter kunt u onbezorgd internetten, toegang krijgen tot uw favoriete sites zonder restricties, en veilig online transacties verrichten.

Uiteraard niet alleen tijdens de vakantie, dit is ook waar voor mensen die veel voor het werk, soms verplicht zijn via open wifi netwerken, of netwerken in hotels online te gaan.

De Voordelen van een Travel Router: Veilig en Voordelig Internetten op Reis

In een tijdperk waarin connectiviteit en digitale veiligheid centraal staan, is de reisrouter een essentiële gadget geworden voor de moderne reiziger. Of u nu op vakantie gaat of voor zaken reist, de mogelijkheid om veilig, privé en voordelig online te gaan, is belangrijker dan ooit. Hieronder verkennen we de voordelen van het gebruik van een reisrouter tijdens uw reizen.

1. Kostenbesparing

Een van de meest directe voordelen van een reisrouter is de aanzienlijke kostenbesparing. Veel hotels, campings en andere accommodaties rekenen per apparaat voor wifi-toegang. Voor een gezin of groep reizigers kunnen deze kosten snel oplopen. Een reisrouter stelt u in staat om met meerdere apparaten - laptops, smartphones, tablets - tegelijkertijd gebruik te maken van één betaalde internetverbinding. Dit betekent dat u slechts voor één apparaat hoeft te betalen terwijl u toch van volledige connectiviteit geniet.

2. Verbeterde Beveiliging

Openbare wifi-netwerken, zoals die in hotels of cafés, staan bekend om hun gebrek aan beveiliging. Dit maakt ze tot een vruchtbare grond voor hackers en cybercriminelen. Een reisrouter, vooral wanneer gecombineerd met een VPN (Virtual Private Network), versleutelt uw internetverkeer en beschermt uw gegevens tegen nieuwsgierige blikken. Het gebruik van een reisrouter is een eenvoudige manier om uw digitale voetafdruk te beveiligen en uw persoonlijke informatie veilig te houden.

3. Toegang tot Geografisch Beperkte Inhoud

Veel landen en organisaties beperken de toegang tot bepaalde websites en diensten. Met een reisrouter kunt u deze beperkingen omzeilen. Door verbinding te maken met een VPN, kunt u uw locatie virtueel veranderen, waardoor u toegang krijgt tot inhoud die anders niet beschikbaar zou zijn in uw werkelijke locatie. Dit is bijzonder handig voor reizigers die toegang willen behouden tot hun favoriete series, nieuwswebsites of sociale mediaplatforms.

4. Eenvoudige Connectiviteit

Reisrouters zijn ontworpen met het oog op gebruiksgemak. Ze zijn klein, draagbaar en eenvoudig in te stellen, waardoor ze ideaal zijn voor reizigers die geen technische experts zijn. Zodra de reisrouter is ingesteld, kunnen alle apparaten met slechts een paar klikken verbinding maken, waardoor u moeiteloos online kunt gaan.

5. Betrouwbare Verbinding

In tegenstelling tot veel openbare wifi-netwerken, die vaak traag en onbetrouwbaar zijn, bieden reisrouters een stabielere en snellere verbinding. Dit is vooral belangrijk voor reizigers die online moeten werken, videoconferenties moeten houden of streamingdiensten willen gebruiken zonder onderbrekingen.

De reisrouter is een onmisbare tool voor iedereen die waarde hecht aan veiligheid, privacy en kostenbesparing tijdens het reizen. Het biedt een veilige haven in de onzekere wateren van openbare wifi-netwerken, terwijl het tegelijkertijd de deuren opent naar een wereld van onbeperkte internettoegang. Of u nu een digitale nomade bent, een vakantieganger of een zakenreiziger, de voordelen van een reisrouter maken het een onmisbaar onderdeel van uw reisuitrusting.

Wat is een Captive Portal?

Een captive portal is een webpagina waarmee netwerktoegang wordt beheerd op openbare Wi-Fi-netwerken, zoals in cafés, hotels, luchthavens of treinen. Wanneer gebruikers verbinding maken met het Wi-Fi-netwerk, worden ze automatisch omgeleid naar deze webpagina voordat ze toegang krijgen tot het internet.

Deze portal kan verschillende doeleinden hebben: het kan gebruikers om inloggegevens vragen, hen verplichten akkoord te gaan met de gebruiksvoorwaarden, of zelfs een betaalproces initiëren voor toegang tot het netwerk.

Waarom wordt een Captive Portal gebruikt?

De belangrijkste redenen voor het gebruik van captive portals zijn veiligheid, regelgeving, en commerciële voordelen.

Veiligheid:

Door gebruikers te verplichten zich aan te melden of een gebruikersovereenkomst te accepteren, kunnen netwerkbeheerders een basishoogte van veiligheid waarborgen en misbruik voorkomen.

Regelgeving:

In sommige landen zijn bedrijven wettelijk verplicht om gebruikersidentificatie te verzamelen voordat ze toegang tot het internet bieden. Captive portals helpen bij het naleven van deze wetten.

Commerciële voordelen:

Bedrijven gebruiken captive portals ook om marketingdoeleinden, zoals het verzamelen van e-mailadressen voor nieuwsbrieven of het tonen van advertenties.

Wie gebruikt een Captive Portal?

Captive portals worden gebruikt door een breed scala aan organisaties en instellingen, waaronder:

Horeca:

Hotels en restaurants bieden vaak gratis Wi-Fi aan hun klanten aan, met behulp van een captive portal om toegang te beheren.

Transport:

Luchthavens, treinen en busstations gebruiken captive portals om reizigers toegang tot het internet te bieden.

Onderwijsinstellingen: Scholen en universiteiten beheren netwerktoegang voor studenten en personeel via captive portals.

Bedrijven:

Sommige bedrijven gebruiken captive portals voor gastnetwerken om de toegang te beheren en het netwerk veilig te houden.

De Evil Twin: Evil Captive Portal

Een "Evil Captive Portal" is een kwaadaardige variant van een captive portal, opgezet door cybercriminelen om gevoelige informatie te stelen of malware te verspreiden. Deze valse netwerken imiteren legitieme openbare Wi-Fi-netwerken, compleet met een captive portal die echt lijkt. Onoplettende gebruikers die verbinding maken met zo'n netwerk en hun inloggegevens invoeren, kunnen slachtoffer worden van identiteitsdiefstal, financiële fraude, of andere cybermisdrijven.

Gevaren van Evil Captive Portals

Phishing:

Gebruikers kunnen worden misleid om persoonlijke informatie, zoals wachtwoorden of creditcardgegevens, in te voeren.

Malwareverspreiding:

Een kwaadaardige portal kan gebruikers ertoe aanzetten malware te downloaden, wat leidt tot verdere compromittering van hun apparaat.

Netwerkaanvallen:

Eenmaal verbonden met het valse netwerk, kan de aanvaller pogingen ondernemen om toegang te krijgen tot het apparaat van de gebruiker of het verkeer te onderscheppen.

Hoe te Beschermen tegen Evil Captive Portals

Wees voorzichtig met openbare Wi-Fi: Vermijd het invoeren van persoonlijke informatie of het uitvoeren van financiële transacties over openbare Wi-Fi-netwerken.

Gebruik VPN:

Een betrouwbare VPN (Virtual Private Network) versleutelt uw internetverkeer, waardoor het veel moeilijker wordt voor aanvallers om uw gegevens te onderscheppen.

Controleer de authenticiteit:

Wees sceptisch over Wi-Fi-netwerken die gevoelige informatie vragen via een captive portal. Controleer bij twijfel de authenticiteit van het netwerk bij de dienstverlener.

Captive portals spelen een cruciale rol in het beheer van netwerktoegang in openbare ruimtes, maar brengen ook risico's met zich mee door de mogelijkheid van kwaadaardige imitaties.

Het is essentieel voor gebruikers om zich bewust te zijn van deze risico's en voorzorgsmaatregelen te nemen om hun informatie te beschermen. Door voorzichtig te zijn met waar en hoe we verbinden met openbare Wi-Fi-netwerken, kunnen we onszelf beschermen tegen de gevaren van evil captive portals en veilig blijven in een steeds meer verbonden wereld.

Bitdefender Total Security

Uw Digitale Schild in het Tijdperk van Cyberdreigingen

In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, is het essentieel om een krachtige, alles-omvattende beveiligingsoplossing te hebben. Bitdefender Total Security staat bekend als een van de meest betrouwbare en geavanceerde cybersecuritysoftware op de markt. Met zijn uitgebreide bescherming tegen allerlei soorten online dreigingen, waaronder virussen, ransomware, phishing, en meer, biedt Bitdefender Total Security een noodzakelijke verdediging voor zowel particuliere gebruikers als bedrijven.

Waarom Bitdefender Total Security?

1. Allesomvattende Bescherming:

Bitdefender Total Security biedt een breed scala aan beveiligingsfuncties, waaronder antivirus, anti-malware, firewall, ransomwarebescherming, online phishingpreventie, en veilig browsen. Deze functies zijn ontworpen om gebruikers te beschermen tegen een verscheidenheid aan cyberdreigingen, zowel bekend als onbekend, dankzij de voortdurende updates en real-time bescherming.

2. Multi-platform Ondersteuning:

Een uniek voordeel van Bitdefender Total Security is de ondersteuning voor meerdere besturingssystemen, waaronder Windows, macOS, iOS en Android. Dit zorgt ervoor dat gebruikers op al hun apparaten beschermd zijn, wat essentieel is in een tijd waarin we meerdere digitale apparaten gebruiken voor zowel werk als privédoeleinden.

3. Prestatie en Snelheid:

Ondanks zijn uitgebreide beveiligingsfuncties, staat Bitdefender bekend om zijn lage impact op systeemprestaties. De software is ontworpen om effectief te werken zonder uw apparaat te vertragen, wat zorgt voor een soepele en ononderbroken ervaring, of u nu aan het werk bent, aan het gamen of gewoon aan het surfen op het internet.

4. Gebruiksvriendelijkheid:

Bitdefender Total Security biedt een intuïtieve en gebruiksvriendelijke interface, waardoor het gemakkelijk is voor gebruikers om hun beveiligingsinstellingen te beheren en aan te passen. Zelfs voor degenen die niet technisch onderlegd zijn, maakt Bitdefender het eenvoudig om optimale bescherming te waarborgen.

5. Aanvullende Functies:

Naast de basisbeveiligingsfuncties, biedt Bitdefender Total Security extra tools zoals ouderlijk toezicht, een wachtwoordmanager, een veilige VPN voor anoniem surfen, en anti-diefstalfuncties voor mobiele apparaten. Deze extra functies bieden een extra laag bescherming en gemak, waardoor gebruikers met een gerust hart online kunnen gaan.

Meer dan Noodzakelijk in de Huidige Digitale Wereld

Met de voortdurende toename van cyberdreigingen is het meer dan ooit noodzakelijk om een betrouwbare beveiligingsoplossing te hebben. Bitdefender Total Security biedt niet alleen bescherming tegen de meest voorkomende dreigingen, maar ook tegen de nieuwste en meest geavanceerde cyberaanvallen. Door te kiezen voor Bitdefender Total Security, kunnen gebruikers vertrouwen op een sterke verdedigingslinie die hun digitale leven beschermt.

In een tijd waarin onze persoonlijke en professionele gegevens voortdurend online staan, is investeren in een robuuste cybersecurityoplossing geen luxe, maar een noodzaak. Bitdefender Total Security staat symbool voor deze noodzakelijke beveiliging, waardoor het een essentiële keuze is voor iedereen die waarde hecht aan hun privacy en veiligheid online.

Wij zetten Bitdefender Total Security breed in op alle apparaten die we gebruiken, inclusief PC's, Macs, en mobiele telefoons.

Deze keuze voor Bitdefender als onze beveiligingsoplossing komt voort uit de uitgebreide bescherming die het biedt tegen een scala aan cyberdreigingen.

Bitdefender Total Security blinkt uit in het beschermen van gebruikers tegen het bezoeken van potentieel gevaarlijke websites en het veilig downloaden van bestanden. Dit omvat zelfs bestanden die op het eerste gezicht onschuldig lijken, zoals foto's, waarbij standaardbeveiligingssoftware mogelijk geen risico's detecteert. Het is een cruciale laag van verdediging in een tijd waarin cyberdreigingen steeds geraffineerder worden.

Hoewel Bitdefender soms als belemmerend kan worden ervaren voor het gebruiksgemak, is dit een indicatie dat de software zijn werk doet door u extra te waarschuwen voor potentieel onveilige handelingen of content. In dergelijke gevallen is het raadzaam om extra voorzichtig te zijn, aangezien Bitdefender mogelijk een probleem heeft geïdentificeerd dat verdere aandacht vereist.

Deze aanpak van proactieve bescherming en het voortdurende streven naar een veilige digitale omgeving maakt Bitdefender Total Security een onmisbaar instrument voor onze dagelijkse online activiteiten. Het zorgt ervoor dat wij, en onze gegevens, beschermd blijven tegen de veelzijdige en steeds veranderende aard van online bedreigingen.

Het Verborgen Gevaar

Bij het online delen en downloaden van foto's ligt een niet direct zichtbaar gevaar op de loer, een thema dat vaak wordt belicht in educatieve video's over cybersecurity.

Deze video's richten zich op het informeren van het publiek over hoe onschuldig lijkende bestanden, zoals foto's, kunnen worden gebruikt als een trojan horse voor malware of andere schadelijke code.

Stel je voor, je ontvangt een e-mail met een foto van een vriend, of je downloadt een afbeelding die je leuk vindt van het internet. Op het eerste gezicht lijkt er niets aan de hand. Echter, in de wereld van cybersecurity, zijn uiterlijke schijn en bestandsextensies niet altijd wat ze lijken. Hackers en cybercriminelen hebben geavanceerde methoden ontwikkeld om malware te verbergen binnen wat lijkt op een onschuldig fotobestand.

Hoe Werkt Het?

De video toont aan dat de techniek achter deze aanvallen steganografie kan omvatten, een methode waarbij gegevens binnen andere bestanden worden verborgen, of het manipuleren van bestandsextensies zodat een uitvoerbaar bestand (.exe) lijkt op een afbeeldingsbestand (.jpg of .png).

Wanneer de gebruiker het bestand opent, wordt de verborgen malware geactiveerd, wat kan leiden tot ongeautoriseerde toegang, datadiefstal, of zelfs ransomware-aanvallen.

Preventieve Maatregelen

De video benadrukt het belang van preventieve maatregelen, zoals:

- Het niet openen van bestanden van onbekende afzenders.
- Het gebruik van betrouwbare antivirussoftware die actief scans uitvoert op gedownloade bestanden.
- Het up-to-date houden van alle software, inclusief het besturingssysteem en applicaties, om bekende kwetsbaarheden te dichten.
- Het educeren van uzelf en anderen over de risico's van digitale communicatie en bestandsuitwisseling.

Het uiteindelijke doel van dergelijke video's is om bewustzijn te creëren over de potentiële gevaren die online op de loer liggen, zelfs in zoiets alledaags als het uitwisselen van foto's. Door te informeren over de methoden die cybercriminelen gebruiken en hoe men zich hiertegen kan beschermen, versterken deze video's de digitale veiligheid en weerbaarheid van individuen en organisaties tegen cyberdreigingen.

Link naar de website

<https://ethisch-hacker.be/hoe-een-foto-gevaarlijk-kan-zijn/>

Wat is Telefoonnummer Vervalsing (Spoofing)?

Telefoonnummer vervalsing, beter bekend als "spoofing", is een techniek waarbij bellers hun telefoonnummer verbergen of vervalsen, zodat op het scherm van de ontvanger een ander nummer wordt weergegeven. Dit kan zijn voor kwaadaardige doeleinden, zoals fraude of spam, maar wordt ook gebruikt voor legitieme redenen, zoals door bedrijven die hun hoofdnummer willen weergeven wanneer verschillende medewerkers bellen.

De technologie achter nummervervalsing maakt gebruik van Voice over IP (VoIP) en specifieke software, waarmee de beller ID-informatie die wordt doorgestuurd naar het netwerk van de ontvanger, kan manipuleren. Hoewel er legitieme toepassingen zijn, zoals privacybescherming of zakelijke doeleinden, wordt spoofing vaak geassocieerd met frauduleuze activiteiten.

De Gevaren van Telefoonnummer Vervalsing

Telefoonnummer vervalsing kan leiden tot verschillende vormen van misbruik en fraude:

Phishing-aanvallen:

Criminelen doen zich voor als vertegenwoordigers van banken, overheidsinstellingen of andere organisaties om persoonlijke of financiële informatie te ontfutselen.

Oplichting:

Door nummervervalsing kunnen oplichters geloofwaardiger overkomen, waardoor mensen sneller geneigd zijn te betalen of persoonlijke informatie te delen.

Identiteitsdiefstal:

Door zich voor te doen als een vertrouwde instantie, kunnen fraudeurs genoeg informatie verzamelen om identiteitsdiefstal te plegen.

Spam en ongewenste oproepen:
Spoofing wordt ook gebruikt om te verbergen waar spamoproepen vandaan komen, waardoor het moeilijker wordt om deze te blokkeren.

Bescherming tegen Telefoonnummer Vervalsing

Hoewel het moeilijk kan zijn om je volledig te beschermen tegen nummervervalsing, zijn er stappen die je kunt nemen om het risico te verkleinen en jezelf te beschermen:

Wees sceptisch:

Ga ervan uit dat oproepen van onbekende nummers of onverwachte oproepen van bedrijven of overheidsinstanties niet legitiem zijn. Verifieer altijd door rechtstreeks contact op te nemen via een officieel nummer of website.

Deel geen persoonlijke informatie:

Geef nooit persoonlijke of financiële informatie over de telefoon tenzij je absoluut zeker weet met wie je spreekt.

Gebruik oproepfiltering:

Veel telefoonmaatschappijen en apps bieden diensten aan om verdachte oproepen te identificeren of te blokkeren.

Meld verdachte oproepen:

Rapporteer spoofing aan je telefoonmaatschappij of lokale autoriteiten. In sommige landen kun je dit soort activiteiten melden bij specifieke overheidsinstanties.

Wees bewust van je rechten:

Informeer jezelf over de wetten en regelgevingen in je land die consumenten beschermen tegen frauduleuze oproepen en telefoonnummer vervalsing.

Telefoonnummer vervalsing vormt een aanzienlijk risico in het digitale tijdperk, met potentieel ernstige gevolgen voor individuen die het slachtoffer worden van fraude en oplichting.

Door op de hoogte te zijn van de methoden die fraudeurs gebruiken en proactieve maatregelen te nemen, kun je jezelf en je persoonlijke informatie beter beschermen. Het is essentieel om altijd waakzaam te blijven, kritisch na te denken over de oproepen die je ontvangt en de juiste stappen te ondernemen om je veiligheid te waarborgen.

Aanvulling op Bescherming tegen Telefoonnummer Vervalsing

Het herkennen van potentieel gevaarlijke situaties is cruciaal bij het beschermen tegen telefoonnummer vervalsing.

Stel, u ontvangt een oproep die zogenaamd van uw bank komt, waarin u wordt gevraagd naar persoonlijke informatie zoals uw geboortedatum en volledige naam, zogenaamd om uw identiteit te verifiëren. De beller beweert dat er verdachte activiteiten op uw rekening zijn gedetecteerd en dringt aan op een snelle online controle, waarvoor u uw bankapparaatje (token) moet gebruiken. In zo'n scenario is het van het grootste belang dat u onmiddellijk ophangt.

Reeds bij de vraag om u te identificeren, moet een alarmbel afgaan. Uw bank heeft al uw gegevens en weet precies wie u bent. Mocht er werkelijk iets aan de hand zijn met uw rekening, dan zal uw bank u doorgaans uitnodigen om persoonlijk langs te komen op kantoor, niet om gevoelige informatie over de telefoon te delen.

Het is ook essentieel om op uw hoede te zijn bij elke oproep van een onbekende beller. Antwoord nooit bevestigend met "ja" als men vraagt of zij spreken met [uw naam] of een variatie daarop. Een betere aanpak is om onmiddellijk te vragen: "Wie bent u en waarom belt u?"

Bovendien, als u een oproep ontvangt van een nummer dat bekend lijkt, maar er is ruis op de lijn of enige vorm van hinder en de beller, die zich voordoet als een vriend, kennis of familielid, vraagt om geld of persoonlijke informatie, hang dan op. Bel niet terug naar het nummer dat zojuist heeft gebeld, zelfs niet als het opgeslagen is in uw telefoon. Het kan een gespoofd nummer zijn dat ontworpen is om u te misleiden. In plaats daarvan, gebruik een bekend en betrouwbaar nummer om contact op te nemen met de persoon in kwestie om de oproep te verifiëren.

Verdere Acties

In het licht van deze aanvullende scenario's wordt het belang van kritisch denken en voorzichtigheid in communicatie nog duidelijker. Het herkennen van de tekenen van telefoonnummer vervalsing en het weten hoe te reageren, is onontbeerlijk in de strijd tegen fraude en oplichting. Door deze praktijken te hanteren, versterkt u uw verdediging tegen potentiële aanvallen en beschermt u uw persoonlijke en financiële informatie tegen misbruik

Wat is VoIP en hoe veilig is het?

Voice over Internet Protocol (VoIP) technologie maakt het mogelijk om spraakcommunicatie en andere communicatiediensten via het internet te laten lopen, in plaats van via het traditionele openbare geschakelde telefoonnetwerk (PSTN).

De veiligheid van VoIP hangt af van verschillende factoren, waaronder de implementatie, het onderhoud en het gebruik ervan. Hier zijn enkele belangrijke punten over de veiligheid van VoIP-technologie:

Encryptie:

VoIP-gesprekken kunnen worden versleuteld, wat helpt om ze te beschermen tegen afluisteren. Protocollen zoals Secure Real-time Transport Protocol (SRTP) en Transport Layer Security (TLS) worden gebruikt om de gegevens te versleutelen en de communicatie veiliger te maken.

Authenticatie:

Sterke authenticatiemethoden helpen bij het verifiëren van de identiteit van gebruikers en apparaten, wat ongeautoriseerde toegang tot het VoIP-systeem kan voorkomen.

Netwerkbeveiliging:

De algemene veiligheid van een VoIP-systeem hangt ook af van de beveiliging van het onderliggende netwerk. Firewalls, intrusion detection/prevention systems (IDS/IPS), en netwerksegmentatie kunnen helpen bij het beschermen van VoIP-systemen tegen aanvallen.

Beheer van kwetsbaarheden: Regelmatige updates en patches voor VoIP-software en -hardware zijn cruciaal om bekende kwetsbaarheden te verhelpen en de beveiliging te handhaven.

VoIP-specifieke bedreigingen: Er zijn verschillende bedreigingen specifiek voor VoIP-technologie, zoals SPIT (Spam over Internet Telephony), vishing (voice phishing), en toll fraud. Het implementeren van adequate beveiligingsmaatregelen is essentieel om deze bedreigingen tegen te gaan.

Afhankelijkheid van de internetservice: Aangezien VoIP afhankelijk is van de internetverbinding, kan de veiligheid en betrouwbaarheid worden beïnvloed door de veiligheidsmaatregelen en stabiliteit van de internetdienstverlener.

Compliance en privacy:

Voor organisaties die onderworpen zijn aan specifieke regelgeving rond privacy en gegevensbescherming (zoals GDPR in Europa of HIPAA in de VS), is het belangrijk om ervoor te zorgen dat hun VoIP-systemen aan deze vereisten voldoen.

Samenvattend, VoIP-technologie kan veilig zijn mits er correcte en doordachte beveiligingsmaatregelen worden geïmplementeerd en onderhouden. Het is belangrijk voor organisaties en individuen om een proactieve benadering te hanteren ten aanzien van de beveiliging van hun VoIP-systemen, door gebruik te maken van sterke encryptie, goede netwerkbeveiligingspraktijken, regelmatige software-updates, en bewustwording van de gebruiker.

En ja, VoIP-gesprekken kunnen potentieel beluisterd worden, via een populaire netwerkprotocol-analyzer die gebruikt wordt voor netwerkdiagnose en analyse, evenals voor onderwijsdoeleinden. Dit programma kan data pakketten op een netwerk onderscheppen en deze informatie gedetailleerd weergeven. Dit houdt in dat als iemand toegang heeft tot het netwerk waarover een VoIP-gesprek plaatsvindt en deze persoon de pakketten kan onderscheppen, hij of zij de data kan analyseren en mogelijk het gesprek kan reconstrueren.

Er zijn echter belangrijke factoren die bepalen of een VoIP-gesprek daadwerkelijk kan worden beluisterd:

Encryptie:

Als VoIP-gesprekken zijn versleuteld met sterke encryptieprotocollen zoals SRTP (Secure Real-Time Transport Protocol) of TLS (Transport Layer Security) voor de signaleringsdata, dan wordt het aanzienlijk moeilijker tot onmogelijk om de gesprekken te onderscheppen en te ontcijferen zonder de bijbehorende encryptiesleutels.

Netwerktoegang:

Een aanvaller of gebruiker heeft toegang tot hetzelfde lokale netwerk (LAN) als de VoIP-apparaten nodig, of moet op een andere manier in staat zijn om de data die tussen deze apparaten wordt uitgewisseld te onderscheppen. Dit kan via man-in-the-middle-aanvallen, toegang tot netwerkapparatuur, of door op een netwerk te zijn waarop port mirroring is ingesteld.

Technische vaardigheden:

Het vereist een bepaald niveau van technische kennis om dergelijk programma effectief te gebruiken voor het onderscheppen en analyseren van VoIP-gesprekken. De gebruiker moet weten hoe hij of zij gefilterde data moet interpreteren en eventueel de audio uit de pakketten moet extraheren.

Het is daarom belangrijk om sterke encryptiemethoden te gebruiken en goede netwerkbeveiligingspraktijken te hanteren om de risico's van het onderscheppen van VoIP-gesprekken te minimaliseren. Daarnaast is het essentieel om op de hoogte te zijn van de privacywetten en -regelgeving in je regio, aangezien het onderscheppen en af luisteren van communicatie zonder toestemming illegaal kan zijn.

Afsluiter

Terwijl we de laatste pagina van deze reis door de wereld van internetveiligheid omslaan, staan we niet alleen stil bij het einde van een boek, maar ook bij het begin van een voortdurende ontdekkingsreis. "Veilig Online: Mijn Reis Naar Digitale Beveiliging" heeft als doel gediend om licht te werpen op de complexe, maar uiterst belangrijke aspecten van onze digitale aanwezigheid. Van de fundamenteën van ethisch hacken tot de geavanceerde strategieën van security management, we hebben samen een pad bewandeld dat rijk is aan kennis, inzicht en praktische adviezen.

Maar de reis stopt hier niet. De wereld van cybersecurity is dynamisch en evolueert voortdurend, gedreven door zowel technologische vooruitgang als de onvermoeibare innovatie van cyberdreigingen. Het is aan ons, als verantwoordelijke digitale burgers, om onszelf uitgerust en alert te houden tegenover de risico's die ons online bestaan met zich meebrengt.

Ik moedig u aan om dit boek niet slechts als een eenmalige leeservaring te beschouwen, maar als een levende bron die u kunt raadplegen, een kompas in tijden van onzekerheid en een springplank voor verdere educatie. Deel uw kennis met anderen, blij nieuwsgierig en blijf leren. Onze gezamenlijke inspanningen in het bevorderen van internetveiligheid kunnen een kettingreactie van bewustzijn creëren, een die sterker is dan welke cybersecuritymaatregel dan ook.

Terwijl we vooruitkijken, ben ik verheugd aan te kondigen dat we werken aan nieuwe boeken die zich richten op de snijvlakken van technologie en veiligheid.

Het ene boek zal de intrigerende wereld van A.I. en hacking verkennen, waarbij we de complexe dynamiek tussen kunstmatige intelligentie en cybersecurity ontwarren.

Het andere boek zal zich richten op veilig werken online door middel van virtuele omgevingen zoals VirtualBox, waarbij we uitleggen waarom deze benadering niet alleen nuttig, maar vooral veilig is.

Beide boeken zijn ontworpen om u te voorzien van de kennis en tools die nodig zijn om te navigeren in de steeds evoluerende digitale landschap.

Ik wil u bedanken voor het vergezellen op deze reis. Moge uw pad voorwaarts veilig, geïnformeerd en beschermd zijn. Laten we samenwerken om een veiliger digitale wereld te bouwen, één klik, één persoon, één moment tegelijk.

Veilig surfen,

Marc

Links

Ons Telegram kanaal



Onze Podcast kanaal



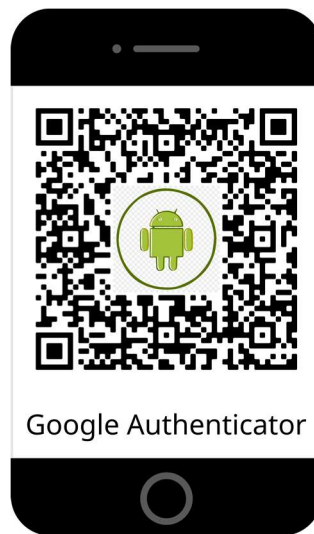
Onze website



Onze Facebook pagina



Link naar de Google Authenticator app



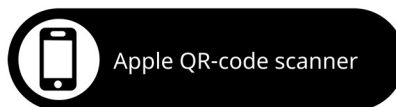
Link naar de iOS versie van Google Authenticator app



Link naar Surfshark website



Link naar de iOS versie van een QR Code preview scanner



Link naar de Android versie van een QR Code preview scanner



Link naar Bitdefender
- Total Security versie -
(met korting)

