Weerbaar op het Web

Uitleg van de termen

Voor meer informatie, of om fraude te melden, ga naar de website van de fraude helpdesk: https://www.fraudehelpdesk.nl/

Adresbalk

Boven in het internetprogramma (browser) is altijd de adresbalk te vinden. Deze neemt het grootste deel van het scherm in en is gevuld met de URL oftewel het adres van de website.

Afzender

De afzender van een e-mail is vaak de persoon of het bedrijf die de mail geschreven en verstuurd heeft. Maar deze namen kunnen vals zijn.
Afzender: Truus de Kat {t.dekat@gmail.com}

Bedrijfsnaam

De bedrijfsnaam moet je meestal kunnen terugvinden als domein. Komt dit niet overeen, dan moeten er gelijk alarmbellen afgaan. Natuurlijk zijn er nog altijd bedrijven die andere services gebruiken om bijvoorbeeld een onderzoek te doen, iets te laten betalen of die een tweede website hebben met een andere naam. Het is daarom geen zekerheid voor crimineel gedrag.

Bijlage

Bij een e-mail is het mogelijk om een bijlage toe te voegen. Dit kan van alles zijn wat met de e-mail wordt meegestuurd. Het is ook mogelijk om als bijlage een virus mee te sturen of een programma dat jouw computer overneemt of je bespioneert. Daarom is het belangrijk om ook een bijlage te controleren vóór het downloaden. Een bestand bestaat uit twee delen, de bestandsnaam en het bestandstype: bestandsnaam.bestandstype Aan het bestandstype, kun je al best veel aflezen: .zip, .exe en .bat zijn bestandstypen die zelf iets kunnen doen als we ze downloaden of aanklikken. Documenten en plaatjes (.doc{x), .pdf, .jp(e)g, .png en .gif) kunnen dat niet.
Criminelen worden steeds slimmer, dus het is altijd een goed idee om alleen bijlagen te openen als jij weet dat ze van een betrouwbare afzender komen, ook voor bestandstypes die betrouwbaar lijken.

Bit.ly (URL-verkorter)

Dit is een voorbeeld van een service die gebruikt wordt om lange URL's te verkorten. Dit kan heel handig zijn, maar het kan ook gebruikt worden om de URL en het domein te verstoppen. De meest gebruikte services zijn: bit.ly, rebrand.ly, tinyURL.com, BL.ink, short.io, snip.ly
Om de verkorte URL terug te vinden, kun je bijvoorbeeld deze site gebruiken: unshorten.it (https://unshorten.it/). Vul op die website de verkorte URL in en de website geeft jou te zien welke lange URL er echt achter zit. Deze URL kan je op betrouwbaarheid controleren.

Domein
Het domein is het belangrijkste deel van de URL of het deel van een e-mailadres dat na het @ komt. Dit is ook hetzelfde als de naam van een site. Bijvoorbeeld nos(.nl) is het domein van de NOS. Google(.nl) is het Nederlandse domein van Google. Dat het Nederlands is kunnen we aflezen uit de .nl extensie. Zie ook URL.
 https://www.voorbeeld.nl/watiseenurl
Een domein klopt als de URL overeenkomt met email en (bedrijfs)naam. Als je het echt zeker wilt weten kan je ook zo het domein invullen. Is dit de website die je verwacht?

E-mail of mail
Een e-mail is een digitale brief of een digitaal bericht. Vaak wordt een e-mail alleen een mail genoemd. Een e-mail bestaat uit verschillende onderdelen, namelijk:

- de naam van de afzender
- het e-mailadres van de afzender
- het onderwerp van de e-mail
- het bericht zelf

Veel e-mails hebben ook links, plaatjes en bijlagen. Een e-mail is niet zo veilig. Net als dat iemand je post ongezien open kan maken, kan dat ook met een e-mail gebeuren.

E-mailadres
Dit bestaat uit twee delen, het deel voor het @ (het apenstaartje) en het deel na het @.
Het deel voor het @ zegt iets over de persoon of de afdeling die de mail gestuurd heeft. Vaak zie je hier de voornaam, achternaam, info en noreply. Die laatste twee komen meestal van een automatische e-mailservice of de technische afdeling. Het deel na het @ heet het domein en laat zien vanaf welke website of e-mailservice de e-mail komt. Veel voorkomende mailservices zijn gmail.com, kpn.nl, ziggo.nl, outlook.com, hotmail.com en upc.nl. Bedrijven sturen e-mails vaak vanaf hun eigen site, het domein is dan bijna hetzelfde als de URL.

Extensie
De extensie is het stukje van de URL dat na het domein komt. Een domein met een extensie (nos.nl) geeft een unieke locatie weer op het internet. Als er een andere extensie gebruikt wordt, is het vaak ook een andere site: nos.com (een Amerikaans communicatiebedrijf) of nos.de (een Duits bibliotheeksysteem) zijn natuurlijk niet hetzelfde als nos.nl.
Zie ook de URL:  https://www.voorbeeld.nl/watiseenurl

Factuur
Veel criminelen sturen een factuur of passen een factuur aan met extra kosten. Kijk daarom altijd goed wat je gaat bestellen en wat je moet betalen, voordat je betaalt. Krijg je een factuur voor iets dat je niet besteld hebt? Dan moet je alles gaan controleren. Dit geldt ook voor berichten van de Belastingdienst of de bank of de gemeente. Ga bij twijfel altijd zelf op zoek naar de o\iciële contactgegevens van het bedrijf waar de factuur vandaan komt en vraag het na. O\iciële instanties sturen ook altijd herinneringen om te betalen en sturen deze vaak zelfs per post. Je kan een e-mail ook altijd een tijdje negeren om te kijken wat er gebeurt.

Inbox
Het scherm van een e-mailprogramma waar alle e-mails binnenkomen.

Link
Een link is een stuk tekst waar je op kan klikken om door te gaan naar een website. Elke link bestaat uit twee delen: een tekst en een URL waar je naartoe geleid wordt. De tekst en de URL hoeven niet hetzelfde te zijn. Een link met de tekst “Google.nl” kan alsnog naar de URL “https://www.bing.nl” gaan. Om de URL te kunnen zien, kan je met de muis boven de link zweven voordat je erop klikt. Dit laat in de meeste gevallen de URL zien, zonder dat je erop hoeft te klikken.
Als je de URL kan zien, kan je deze controleren en weet je naar welke website hij gaat
op deze link om de betaling Daarna wordt uw bestelling
https://www.voorbeeld.nl/watiseenurl

Logo en stijl
Hoe netter een website eruitziet, hoe meer reden er is te denken dat het een echte website is. Het kost veel moeite en kennis om een goede website te maken. Een investering die veel criminelen niet willen doen. Stijlen en logo’s kunnen wel gestolen worden. De criminelen worden steeds slimmer, dus het is geen volledige zekerheid.

Phishing
Een bericht waarin een crimineel zich voordoet als iemand anders of als bedrijf. En zo probeert om jouw informatie te krijgen. Phishing komt ook voor als berichtjes via de telefoon of soms zelfs als telefoongesprek. Het is verstandig om bij phishing de o\iciële website te controleren. Doe dit niet via het bericht, ga zelf naar de o\iciële website. Gebruik hiervoor een zoeksite als Google of Bing. Op de o\iciële website staan contactgegevens die je kan gebruiken om na te vragen. Gebruik nooit de contactgegevens uit de e-mail, berichten of het telefoongesprek zelf, want als het criminelen zijn hebben ze deze natuurlijk aangepast.

Slotje
Als er een slotje in de adresbalk staat, is de website beter betrouwbaar. Het slotje betekent dat de website een veiligheidscertificaat heeft die door een betrouwbare partij is goedgekeurd. Omdat sites automatisch gecontroleerd worden, is het gevaar nog niet helemaal geweken. Een valse website kan nog altijd een certificaat bezitten en een slotje krijgen.
https://www.voorbeeld.nl/watiseenurl

URL

De URL is het adres van de website waar je heen gaat als je bijvoorbeeld op een link klikt, of google.nl intypt. Hoe eenvoudiger de URL, hoe veiliger jij je kunt voelen, want er is minder om iets te verstoppen. Merk op dat soms ook URL's best wel lang zijn en veel informatie kunnen bevatten. Het is daarom van belang dat je in een URL het domein kan vinden. Een URL bestaat uit 5 delen:

- Protocol: https://
- Subdomein: www
- Domein: naam van de site
- Extensie: bijvoorbeeld .nl of .com
- Server Informatie: /informatie

Alles na de eerste / kan je negeren als je een URL controleert. Dit is niet van belang voor de betrouwbaarheid. Wat er nog overblijft zijn de delen subdomein, domein en extensie.

 https://www.voorbeeld.nl/watiseenurl

Vaak wordt er in het subdomein gerommeld om mensen op het verkeerde been te zetten. Daarom willen we ook die niet meenemen als we een URL controleren. Het gaat echt om het domein en de extensie. Deze kan je vinden door na https:// op zoek te gaan naar de eerste / . Vanaf deze / ga je 2 punten terug. Tussen deze twee punten staat het domein en na de laatste punt voor de / staat de extensie. De laatste 2 punten voor de eerste / (na https://) is de locatie van het daadwerkelijke domein van de website.

https://www.voorbeeld.nl.nepsite.nl/watiseenurl Of een ander voorbeeld:

www.nos.nl is de site van de NOS. news.nos.nl

kan naar een andere site gaan.

Ww.nos.nl is ook een ander adres en kan ook haar een andere site omgeleid zijn. Het domein en de extensie moet je tenslotte goed op taalfouten controleren. Is dit echt hetzelfde woord of dezelfde naam als verwacht? Voorbeeld: google.nl of gooogle.nl of googl.nl

Het stuk na de eerste / is extra informatie die meegegeven wordt aan de website. Deze informatie heeft een heel laag risico onbetrouwbaar te zijn, je mag alles na de eerste / negeren. Wees altijd extra voorzichtig met een domein waar bit.ly of een rebrand.ly in staat. Deze kunnen worden gebruikt om een andere URL te verstoppen.