CYBER SECURITY

Inleiding tot de gevaren op het internet

Cybercriminelen gebruiken verschillende methodes om jullie huiskamer binnen te dringen. 90% van alle cyberincidenten begint ?

- Bij de spamfilter ?
- Aan de Firewall?
- Door menselijke fout?

Waarom is security awareness zo belangrijk?

Ik bescherm zo:

- Mijzelf en mijn gegevens
- Mijn familie
- Mijn vrienden en kennissen !

Wachtwoorden – sleutel tot succes of niet…

VRAAGJE: Hoeveel verschillende wachtwoorden gebruik je best ?

- Voor ieder account hetzelfde paswoord ?
- Twee verschillende wachtwoorden ?
- Voor ieder account een ander wachtwoord ?

Wachtwoorden – sleutel tot succes of niet…

Hoeveel verschillende wachtwoorden gebruik je best ?

- Voor ieder account een ander wachtwoord !

Als één account gehackt wordt, zijn de andere accounts nog veilig! Hackers proberen met het gevonden paswoord alle gekende websites uit in de hoop op meerdere platformen binnen te geraken = ‘Credential Stuffing’

Wachtwoorden – sleutel tot succes of niet…

VRAAGJE: Uit hoeveel tekens moet je wachtwoord minstens bestaan?

- 7 tekens ?
- 9 tekens ?
- 14 tekens ?

Sterke wachtwoorden zijn vooral LAAANG

Hoe lang doet een hacker erover om volgende wachtwoorden te kraken:

- azerty -> onmiddellijk
- iloveyousomuch -> meer dan 4 jaar
- myfishisinthewater -> 3000 jaar

Veilig inloggen: nog beter dan wachtwoorden...

Via 2FA = tweefactor-authenticatie

- Je ontvangt via sms een verificatiecode
- Op je smartphone, met een speciale 2FA-app, krijg je een bevestigingscode (bijv. itsme, diverse Authenticatoren,..)

Updaten en backuppen!

VRAAGJE: Als je een melding krijgt voor een update, wat doe je dan best:

- Niets, ik let nooit op updates ?
- Ik voer ze uit voor ik die dag mijn computer afsluit ?
- Ik wacht tot er enkele verschillende updates klaarstaan en voer ze dan allemaal in één keer uit ?

Een back-up is een copy van jouw gegevens (foto's, muziek, bestanden) en bewaar je best op verschillende plaatsen en op verschillende manieren (externe datadragers)

Onderzoek van binnenkomende info!

VRAAGJE: Welke URL (**Uniform Resource Locator**) is niet verdacht:

- www.microsoft.pro
- www.microsoft.com
- www.micr0soft.com

Onderzoek van binnenkomende info!

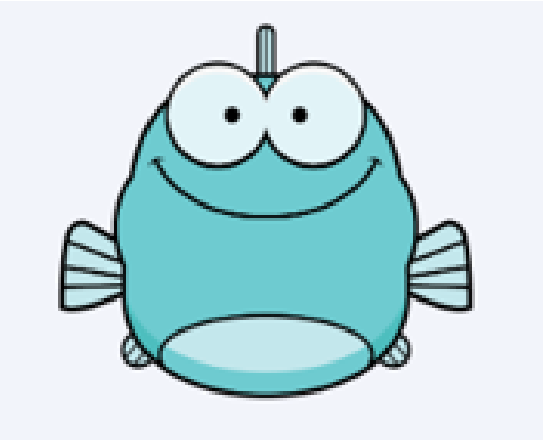
VRAAGJE: Als je een bericht krijgt dat je een gratis smartphone hebt gewonnen...

- ... klik je onmiddellijk op de link. JOEPIE ?
- ... stuur je het door naar familie zodat zij ook kans maken ?
- ... delete je het of stuur je het door naar een IT-professiona

  want je vindt het maar verdacht ?

DE 5 BASISREGELS VAN SECURITY AWARENESS

1. Zorg voor veilige paswoorden (lang, meerdere)
2. Doe je updates
3. Gebruik een goede virusscanner
4. Maak regelmatig een back-up
5. Eerst checken, dan klikken !



Vuistregels om vanaf nu toe te passen

- Klik nooit zomaar op een link en open nooit zomaar een bijlage
- Gebruik geen openbare WiFi (= niet beveiligd)
- Steek geen USB-stick in je computer als je de afzender niet kent
- Gebruik altijd unieke wachtwoorden en maak ze zo lang mogelijk ->

  een wachtwoordzin is ideaal, gecombineerd met tekens
- Ga nooit zomaar in op een vraag geld over te maken of een dringend probleem op te lossen, zelfs niet voor een (op het eerste zicht) bekende of familielid, neem altijd eerst PERSOONLIJK contact op!

Een oefening:

Wat is er verdacht aan dit bericht :

- Het aanbod is niet realistisch ?
- De URL klopt niet ?
- Het e-mailadres van de HR-dienst klopt niet ?
- Het uur ?
- De datum ?
- De aanspreking is onpersoonlijk ?
- Dringendheid van het bericht ?

WHITE WHAT ?

Wat doet een White Hat Hacker :

- Breekt illegaal in computernetwerken in voor eigen gewin ?
- Hackt een computernetwerk van een bedrijf met hun toestemming ?
- Werkt met organisaties om hun veiligheid te verbeteren ?

WHITE WHAT ?

Wat doet een White Hat Hacker :

- Breekt illegaal in computernetwerken in voor eigen gewin ?

☑ Hackt een computernetwerk van een bedrijf met hun toestemming ?

☑ Werkt met organisaties om hun veiligheid te verbeteren ?

Wij noemen dit een ETHISCHE HACKER

HMMM cookies...

Je bezoekt een website en moet al direct vanalles lezen en jouw goedkeuring geven.... De cookies! Maar wat zijn dat ?

- [x] Kleine databestanden die de browser opslaat om mijn online-ervaring aangenamer te maken
- [x] Kleine virussen die websites op mijn computer installeren om zoveel mogelijk informatie te stelen

Wat staat er in een cookiebeleid ?

- Hoe de website mijn gegevens bewaart
- Waarvoor de website mijn gegevens gebruikt
- Wat er gebeurt wanneer ik niet akkoord ben
- Hoe ik mijn keuze kan aanpassen
- Dat je het recht hebt om ‘vergeten te worden’

Door de cookies geef je veel info prijs over je surfgedrag, waarop websites o.a. hun aanbod kunnen afstemmen. Helaas kan je de ‘essentiële cookies’ niet weigeren...

Wat is het gevolg/gevaar van online shoppen ?

- Na een aankoop krijg je via verschillende kanalen reclame voor iets gelijkaardigs (cookies!) Je merkt dat alle platforms met mekaar ‘praten’
- Als je een profiel aanmaakte met betalingsgegevens, komen deze automatisch beschikbaar bij een volgende aankoop… Opgelet dan met meerdere gebruikers van dezelfde computer / GSM of bij hacking
- Je gegevens kunnen doorverkocht worden aan andere partijen
- Oplichting door transportfirma’s wordt moeilijker te herkennen

Valse berichten herkennen: alarmbellen Phishing

- Het aanbod of het bericht is niet realistisch (erfenissen online te verdelen, prijs gewonnen, ...)
- Het is onverwacht (bijv. prijs gewonnen zonder aan iets mee te hebben gedaan, niets besteld)
- Hoogdringende actie vereist
- Aanwezigheid van een link (website, document, ...)
- Afzender is voor jou onbekend (dikwijls een raar mailadres)
- Geen aanspreektitel of een zeer onpersoonlijke aanhef

! Lay-out van gebruikelijke leveranciers wordt tegenwoordig goed nagemaakt

Valse berichten herkennen: wat kan ik zelf checken?

- Surf (bijv. bank, websites zoals Zalando, Paypal, Bol.com, ...) via de normale weg en niet via de aangeboden link
- Log in via de normale weg en niet via de aangeboden link
- Contacteer de hulplijn van de leverancier/bank via het nummer op de website en niet via het nummer in het verdachte bericht
- Contacteer de afzender via telefoon, niet via het verdachte bericht
- Als iemand een nieuw nummer doorgeeft, bel deze dan even op om dit te controleren. Probeer ook het ‘oude’ nummer als je geen contact krijgt!

EHBO help, ik heb verkeerd geklikt

- Verzamel zoveel mogelijk gegevens van het incident:
  - Naam, telefoonnummer, betaling?, ...
- Meld je zo snel mogelijk bij de politie (afspraak maken)
- De officiële instelling (bank, bedrijf) informeren dat hun naam misbruikt wordt
- Betaling met Visa ? -> Visa en bank contacteren

Ook opgelet met HOAX (desinformatie) -> nieuwsgierig -> ...

Wist-je-dat-jes ?

- Ook in je privé-communicatie moet je omzichtig omspringen met de mailadressen van contactpersonen. Als de groep groot is of er is risico op verder doorsturen, gebruik liever BCC in plaats van CC
- Phishing berichten bevatten intussen bijna geen spelfouten meer en bootsen lay-outs van grote websites bijna perfect na en kunnen vanuit mailadressen van bekenden mails fabriceren
- Heb je toch per ongeluk ingelogd op een ‘vreemde’ website, verander onmiddellijk je paswoord en log overal uit.

Niet enkel jouw computer of at random!

- SMISHING = SMS of WhatsApp-phishing
- VISHING = phishing via een telefoongesprek (bank belt om ...)
- SPEAR PHISING = gericht, met info uit social media
- WHALING = doel is CFO, CEO door ‘werknemer met probleem’
- CEO-fraude = uit naam van CFO, CEO mails gestuurd

CYBER SECURITY

Bedankt voor jullie aandacht !

Blijf alert...