Veiligheid & samenleving

Als het goed is heb je de presentatie Veiligheid & Samenleving gevolgd. Tijdens deze presentatie zijn een aantal belangrijke onderwerpen aan bod gekomen, over hoe je veilig kunt deelnemen aan de digitale wereld. Deze hand-out vat de belangrijkste punten uit de presentatie kort samen.

Wat weten we nou echt?

Media pakken tegenwoordig groots uit bij nieuws over virussen, spyware en onder andere hacks. Men wordt bang gemaakt en mensen die niet alle feiten kennen worden angstig, maar weten niet hoe het echt zit.

Het politievirus? Wie heeft ervan gehoord en wie weet daadwerkelijk wat het is? Als je besmet bent met dit computervirus, kom je bij het opstarten van je computer niet terecht in je gebruikelijke omgeving. In plaats daarvan zie je een pagina waarop staat dat je iets fout hebt gedaan en geld moet betalen om de blokkade op te heffen. Je computer wordt als het ware 'gegijzeld'.

De SSH heartbleed bug, wat was het nou precies? Dit was een beveiligingslek op sommige servers die een bepaald type software draaiden. Middels dit lek konden kwaadwillenden data achterhalen die op die server stond. Men heeft ooit gehoord dat een e-mailbijlage gevaarlijk kan zijn, maar weet niet dat dit inmiddels weinig meer voorkomt, en dat geïnfecteerde websites met een drive-by-download veel vaker voorkomen.

Conclusie, men is angstig, hoort van alles, maar is nog niet goed op de hoogte met wat er nou echt aan de hand is.

Virus of malware?

Wat is nou eigenlijk een virus? Of is het malware? Of een Trojaans paard? We spreken tegenwoordig over malware, dit komt van malicious software. Daaronder vallen diverse categorieën. Een specifiek 'virus' bestaat dus niet echt. Overigens is dit een selectie en zijn er in realiteit nog veel meer categorieën. Bijvoorbeeld een rootkit, dit is een set software die wordt gebruikt door derde partijen, nadat er toegang verkregen is tot het systeem.

Hoe veilig ben jij?

Is jouw virusscanner actueel en werkend? In het artikel in PC-Active 278 "De 10 uur van een virus" wordt uitgelegd waarom een virusscanner zo hard nodig is. Het is onverantwoord om nog zonder antivirusoplossing online te zijn. Voor een adware-besmetting en zelfs soms spyware is alleen een gratis standaard antivirus onvoldoende. Je zult dan en extra scanner moeten downloaden.

Stel je bent helemaal beveiligd met een goed antiviruspakket, dan kun je nog steeds iets verkeerds doen. Heb je wel eens gedacht aan je wachtwoord veiligheid? Uit onderzoek komt naar voren dat nog veel mensen wachtwoorden nemen zoals de naam van hun kind. Of erger, welkom01. Een sterk wachtwoord is in deze tijd echt een noodzaak. Systemen worden aan elkaar gekoppeld en we plaatsen steeds gevoelige informatie online. Neem liever een lange zin als wachtwoord en gebruik niet voor elke website het zelfde wachtwoord. Mocht iemand je wachtwoord raden, dan heeft deze persoon of hacker ineens toegang tot alle beveiligde omgevingen. Maar hoe onthoud je dan al die verschillende wachtwoorden, die ook nog eens moeten bestaan uit een aantal woorden, liefst hoofdletter, cijfer en speciaal teken?

hcc!

Je kunt de wachtwoorden gewoon onthouden, als je een goed geheugen hebt. Gelukkig zijn er ook diverse goede (wel betaalde) applicaties die je daarbij kunnen helpen. Dit zijn applicaties die een soort virtuele kluis voorstellen. Je hebt één meestercode (die echt niet te raden is) en deze geeft toegang tot je wachtwoorden. Wat ook steeds meer opkomt is twee-staps-verificatie. Je vult je wachtwoord in en je krijgt ook een code op je mobiel toegestuurd. Die code moet je dan weer op de website invullen. Dit is erg veilig want stel dat je wachtwoord geraden wordt, of erger via een keylogger ontfutseld is, dan komen hackers nog niet in je account, omdat ze niet jouw mobiel hebben.

Identiteitsfraude

Het is eigenlijk het stelen van iemands identiteit en dat is tegenwoordig vrij makkelijk. Je ziet het wel eens: iemand heeft zijn rijbewijs gehaald en zet een foto van zichzelf met rijbewijs op Facebook of een ander online platform. Diegene realiseert zich niet dat er met naam + achternaam, documentnummer en burgerservicenummer heel veel dingen te doen zijn, zeker in combinatie met een kopie van het document!

Denk bijvoorbeeld aan het afsluiten van een lening, bestellen van een mobieltje met abonnement etc. Wat ook kan is dat je zelf niet gegevens online zet, maar dit onbewust doet omdat je denkt dat een legitieme organisatie dit van je wilt weten. Denk aan een bank of creditcard maatschappij. Zie het verhaal van PostNL. (http://www.postnl.nl/over-postnl/pers-nieuws/nieuws/2014/oktober/postnl-waarschuwt-voor-nep-emails.html)

Phishing

In juni 2014 was 1 op de 496 verzonden e-mails een phishing-mail. Social media worden steeds vaker ingezet voor phishing, maar in beperkte mate voor banken. Circa 30% van phishing-aanvallen richt zich op financiële instellingen. Het is een groot gevaar omdat het voor de crimineel zeer lucratief is!

Hoe herken je phishing?

- De e-mail is niet aan de ontvanger persoonlijk gestuurd en begint dus vaak met een algemene opening en aanhef.
- De e-mail bevat vaak taal- en schrijffouten. Het gaat om een slecht stuk vertaalde tekst.
- Er wordt vaak gesuggereerd dat het account "geverifieerd" of te wel gecontroleerd moet worden. Dit controleren moet dan door ergens in te loggen met je (bank)gegevens.
- Er wordt gedreigd dat als men niet inlogt er geen gebruik meer van je bankrekening kan worden gemaakt of dat er een veiligheidsrisico is.
- Het afzender e-mailadres is niet altijd dat van je bank. Vaak word wel een deel van de naam van de bank genoemd.
- Check altijd de URL (https) en de naam!

Vaak denkt men dat je in veel gevallen je gegevens moet achterlaten, maar in veel gevalle n hoeft dat helemaal niet. Als het dan toch moet, denk dan na over welke gegevens je achterlaat. In het geval van

een paspoort of rijbewijs kun je de anti-identiteitsfraude-cover gebruiken, deze is bij veel gemeentes gratis af te halen. Deze cover verbergt je BSN, documentnummer en gegevensstrip.

Schrijf op de kopie:

1. dat het een kopie is
2. voor wie of welk product hij bedoeld is
3. de datum waarop u hem afgeeft

Internetbankieren

Hoe veilig is internetbankieren? Op zich veilig mits aan een aantal voorwaarden wordt voldaan. Je moet een goed antiviruspakket hebben en alle recente software-updates geïnstalleerd hebben. Banken berekenden vroeger het aantal incidenten op basis van echte gemelde zaken. Tegenwoordig nemen banken alleen zaken op in de statistieken, waarbij de gebruiker zelf niets te verwijten viel. Bij incidenten waarbij de gebruiker zelf bijvoorbeeld geen antivirus pakket had/heeft of zelf in een phishing-mail is getrapt, worden de incidenten niet meer meegenomen. Er is ook een verandering in het beleid van banken om in die zaken ook niet zomaar meer het slachtoffer schadeloos te stellen.

In PC-Active 278 staat een artikel over veilig internetbankieren in de box. Deze kun je als achtergrond nog even nalezen.

Contactloos betalen

Het contactloos betalen. Dit geschiedt door middel van NFC en lijkt een beetje op de vervanger van de ChipKnip. Hier hoefde immers voor kleine bedragen ook geen pincode ingevoerd te worden. Als jouw pinpas geschikt is voor contactloos betalen zit er een logo op dat veel weg heeft van het wifi-logo. Probeer het eens uit!

Samenvatting

- Over het algemeen zeer weinig juiste kennis over virussen.
- Virusbeveiliging is een must.
- Je identiteit is zeer waardevol
  Ga er ten alle tijden voorzichtig mee om!
- Phishing is erg lucratief.
- Controleer altijd de website op echtheid.
- Bij twijfel, niet doen!
- Contactloos betalen, vervanging van de ChipKnip.
- Stel je limieten in bij de bank of ga akkoord met standaard limiet.

Bij wie ben je welkom met vragen over alles wat digitaal is?
En hoe zorgen we dat de belangen van digitale consumenten gehoord én behartigd worden?

Het antwoord is hcc

We helpen onze leden graag en bieden veel voordeel.

- **Voordelen en aanbiedingen**
  Als lid ontvang je exclusieve voordelen en aanbiedingen. Waaronder 10% korting op de digitale fotoservice van fotofabriek.nl (incl. gratis verzending) en tot 10% korting op collectieve verzekeringen bij OHRA.

- **6x per jaar PC-Active**
  PC-Active is het grootste computermagazine van Nederland en België over het digitale leven. Het magazine is onderdeel van het lidmaatschap en valt zes keer per jaar automatisch bij alle leden op de mat.

- **Regio's**
  Als HCC-lid word je automatisch ingedeeld in een Regio. Hier worden regelmatig bijeenkomsten georganiseerd over allerlei onderwerpen, regelmatig in samenwerking met de Interessegroepen van HCC.

- **Interessegroepen**
  Je kunt je als lid aanmelden bij één van de vele Interessegroepen. Elk van deze groepen houdt zich bezig met een specifiek onderwerp, zoals Apple, open source, games of beleggen.

- **HCC!forums**
  Op HCC!forums ben je welkom met al je vragen. Kan de vraag niet beantwoord worden door een ander HCC-lid? Dan helpt één van de moderatoren je op weg.

- **HCC!hulp helpdesk**
  Je kunt als lid tegen gereduceerd tarief gebruikmaken van de telefonische helpdesk. Of sluit voor € 6,05 extra per maand een Plusabonnement af en bel met de helpdesk tegen interlokaal tarief.

- **Kwartaalthema's**
  Ieder kwartaal staat er een ander thema centraal bij HCC. Er worden door het hele land themapresentaties gegeven. Daarnaast kun je online terecht voor informatie in de vorm van stappenplannen of filmpjes.

Word nu lid met € 10,- korting!
Voor slechts **€ 27,50** i.p.v. € 37,50
www.hcc.nl/lidworden