**Presentatie Cybercrime: Avondsessie (28-03-2017)**

**Organisatie: CCV/PVO**

**Spreker: Paul de Vlieger, directeur** [www.DigitaleOpsporing.nl](http://www.DigitaleOpsporing.nl)

**Locatie: De Kokerij, Langeweg 16, Oostvoorne**

Hartelijk dank voor uw aanwezigheid op de ondernemersbijeenkomst van 28 maart jl. Wij hopen dat u het net als ons, een geslaagde bijeenkomst heeft gevonden.

Graag sturen wij u met deze hand-out een samenvatting van de belangrijkste tips en aanbevelingen.

|  |
| --- |
| **Algemene tips voor uw online veiligheid** |
| * Installeer en update altijd uw internet beveiligingssoftware.
* Wordt u in een e-mail verzocht op een link te klikken:

1a. Houdt uw muis stil op de link. Het adres waar de link naartoe leidt wordt nu zichtbaar.of1b. Open uw webbrowser, typ de link handmatig in.1. Controleer certificaat van de website. Zgn. SSL certificaat.
* Verwacht u geen bijlage in een e-mail of eindigt de bestandsnaam van de bijlage op een dubbele extensie (zoals bijvoorbeeld .pdf.zip), klik er dan niet op.
* Ben altijd voorzichtig met het openen van .zip en .exe bestanden. Het zgn. cryptolocker virus schuilt vaak in dit soort bestanden.
* Bevat een ontvangen e-mail van een gerenommeerd bedrijf grammaticale fouten, ben dan op uw hoede voor phishing.
* Installeer te allen tijde de updates voor uw besturingssysteem en vermijd het gebruik van illegale software.
* Goede “gratis” virusscanners zijn zeer schaars. Er zijn goede virusscanners te verkrijgen voor € 30,- per werkstation, zoals ESET, Kaspersky en bitdefender.
* Ben voorzichtig indien u gebruik maakt van niet beveiligde, openbare/publieke WiFi-netwerken.
* Verifieer met wie u online communiceert.
* Bij gebruik van Facebook (of andere social media sites): Let op uw privacy instellingen!
* Bij online telebankieren: Vergewis u ervan dat er in de adresregel binnen uw internet browser altijd https://……. staat. Staat dit er niet, log dan niet in. Op de website [www.veiligbankieren.nl](http://www.veiligbankieren.nl/) kunt u meer tips vinden m.b.t. veilig internet bankieren.
* Laat uw website of IT-omgeving in het kader van de nieuwe wetgeving datalekken geregeld controleren door middel van een penetratietest. Indien u hierover meer informatie wenst te ontvangen dan kunt u ons een e-mailbericht sturen of telefonisch contact opnemen.
* Een handig hulpmiddel voor het veilig opslaan van al uw wachtwoorden is bijvoorbeeld Lastpass. Op [www.lastpass.com](http://www.lastpass.com) kunt u informatie vinden.
* Encryptie toepassen op uw PC of laptop is verstandig. Indien de laptop gestolen of verloren wordt heeft er niemand toegang tot uw data die op uw apparaat staat. Google naar bitlocker voor meer informatie.
 |

### **Besproken websites:**

### **Google:**

Een zeer bekende en wereldwijd meest gebruikte zoekmachine. Google ondersteunt naast de normale zoekactie ook geavanceerde zoekacties. Zoeken in/naar openbare broncode, video, blogs, discussiegroepen, boeken en news. Daarnaast is er ook een geografische mogelijkheid (maps), een vertaalpagina en de mogelijkheid om alerts in te stellen. Met google kunt U ook foto’s nakijken op authenticiteit.

* [www.google.nl](http://www.google.nl)

**Google Alerts:**

Hier kunt u alarmmeldingen instellen voor naam, creditcard, bedrijf enz. Hiermee wordt u 24/7 op de hoogte gehouden als uw ingestelde (tref)woorden nieuw op het internet worden gevonden. Vergeet niet de zoekopdracht tussen “ ” te zetten.

* <https://www.google.com/alerts>

### **Waybackmachine:**

Met de Waybackmachine kunt u bekijken hoe websites er in het verleden uit zagen. Dit kan handig zijn wanneer u bijvoorbeeld op zoek bent naar contact gegevens.

* <http://archive.org/web/>

### **Threat-cloud map:**

Via de onderstaande link worden cybercrime aanvallen in kaart gebracht die op dat moment plaatsvinden.

* <https://www.threat-cloud.com/ThreatPortal/#/map>

### **Bewustwordingscursus:**

Via onderstaande link kunt u uw eigen cyber bewustzijnsniveau testen.

* [www.alertonline.nl](http://www.alertonline.nl)

**Alternatieve zoekmachines:**

Probeer eens een andere zoekmachine te gebruiken. Er zijn privacy neutrale zoekmachines.

* [www.duckduckgo.com](http://www.duckduckgo.com)
* [www.ixquick.com](http://www.ixquick.com) (Nederlandse privacy neutrale zoekmachine)
* [www.zoekhulp.nl](http://www.zoekhulp.nl) (verzamelsite voor zoekmachines)

|  |
| --- |
|  **“Wat kan ik morgen aan mijn ICT leverancier vragen?”** |
| * Vraag uw IT leverancier of de laatste beveiligingsupdates door hun geïnstalleerd zijn.
* Vraag uw IT leverancier of ze de backups van uw systeem geregeld controleren of deze geslaagd zijn. Vraag eventueel zelf eens een restore aan van een bestand van een dag eerder ter controle.
* U kunt logfiles opvragen van bijvoorbeeld uw firewall. Daaraan kunt U zien of uw netwerk aangevallen wordt door hackers.
* Laat uw virusscanner controleren of deze bijgewerkt is en of deze voldoende werkt.
 |

## **Heeft u al nagedacht over:**

1. Internet en data protocol;
2. Training medewerkers;
3. Digitale bewustwording op werkvloer;
4. Digitale bewustwording bij directie;
5. Reguliere externe audits.

Bedankt voor uw aandacht en interesse.

Indien u vragen heeft of nadere info wenst, kunt u te allen tijde contact met ons opnemen.