

Interesse in een Human Firewall?

# Hoe herken je de cybercrimineel



## 1. DIEV Introductie

## 2. Vormen van Cybercrime

### 2.0. Introductie

#### 2.1. Phishing

- Wat is phishing
- Soorten phishing
- Phishing herkennen
- Phishing voorkomen & Wat als je met phishing te maken krijgt

#### 2.2. Virussen

- Introductie
- Virussen herkennen
- Virussen voorkomen

#### 2.3. Internetplichting

- Introductie
- Internetplichting herkennen en voorkomen

#### 2.4. Hacking

- Hacking

#### 2.5. Identiteitsfraude

- Introductie
- Identiteitsfraude herkennen en voorkomen

## 3. Data

### 3.1 Introductie

- Data en persoonsgegevens
- Wat is de AVG?

### 3.2. Persoonsgegevens

- Persoonsgegevens en bijzondere persoonsgegevens
- Verwerken van persoonsgegevens (AVG)
- Verwerken van bijzondere persoonsgegevens (AVG)
- Regels voor het verwerken van het burgerservice-nummer
- "Adequate Beveiliging" van persoonsgegevens (AVG)
- Technische en Organisatorische maatregelen (AVG)

### 3.3. Oeps! Een Datalek

- Wanneer spreek je van een datalek?
- Hoe ontstaat een datalek?
- Wat te doen bij een datalek?
- Hoe weet je of jouw gegevens zijn gelekt?

### 3.4. Risico's van een datalek

- Wat zijn de risico's / gevolgen van een datalek?
- Het echte gevaar: meerdere datalekken gecombineerd

### 3.5 Hoe voorkom je een datalek?

- Wat kun jij doen om een datalek te voorkomen?
- Testvragen: Is dit een datalek?

## 4. Wachtwoorden

### 4.1. Introductie

- Veel gemaakte fouten bij het verzinnen van een wachtwoord
- Wat maakt een wachtwoord veilig?
- Volg deze stappen om een veilig wachtwoord te verzinnen!

### 4.2. Een ander wachtwoord voor elk account

- Tips voor het verzinnen en bedenken van verschillende wachtwoorden
- Wachtwoordmanagers
- Wachtwoorden opschrijven?!

### 4.3. Tweestapsverificatie

- Wat is multi-factor-authenticatie (MFA)?
- Waarom is MFA zo veel veiliger?
- Mogelijke stappen binnen MFA
- Risico's van MFA: Hoe houd je het veilig?

## 5. Social Media

### 5.1. Introductie

- Social media is leuk! Maar kent ook risico's
- Waar wordt jouw data voor gebruikt/misbruikt

## 5.2. Wat deel je met wie?

- Welke gegevens zet je op je profiel?
- Wat post je op social media?
- Welke informatie deel je wellicht onbewust?
- Met wie deel je? Standaard instellingen en per post
- Pas op met wie je als "vriend" toevoegt
- Professioneel social media: houd zakelijk en privé gescheiden

## 5.3. Veilig Social Media: 5 praktische tips

- Wie kan jou taggen?
- Phishing via Social Media
- Winacties en advertenties
- Login with Facebook-knop
- Controleer regelmatig je privacy instellingen

## 6. Mobiele Apparaten

### 6.1. Inleiding: Gegevens, virussen en andere uitdagingen

- Waarom cybercriminelen uit zijn op jouw smartphone
- De huidige problemen en uitdagingen in smartphonebeveiliging
- Virussen op je smartphone - Bestaan die?
- Hoe komt malware op jouw smartphone terecht?
- Is een iPhone veiliger dan Android?

### 6.2 Technische beveiligingsopties

- Enterprise Mobility Management
- Mobile Device Management
- Mobile Application Management
- Enterprise App-Store
- Mobile Content Management
- Mobile Threat Defense
- 5 Tips voor een veilig smartphone gebruik

### 6.3 Applicaties en toegang jouw gegevens

- Welke apps geef je toegang tot welke gegevens?
- 3 soorten gegevens op je smartphone
- Wat gebeurt er als je de toegang tot bepaalde gegevens weigert
- 3 risico's bij het gebruiken van apps
- Gevolgen van het (ongewenst) delen van te veel informatie

### 6.4 7 tips voor veilig gebruik van applicaties

## 7. Werken op Locatie (thuis, ergens anders)

### 7.1. Introductie

- De uitdagingen rondom het thuiswerken
- Werken op locatie: is dat veilig?

### 7.2. Veilig thuiswerken

- 4 tips voor een veilig thuisnetwerk
- Veilig communiceren vanuit huis
- Welk programma gebruik je?
- Wat is er in beeld tijdens een videocall?
- Wat deel je op je scherm tijdens een videocall?

### 7.3. Veilig werken op afstand

- De gevaren van Free WiFi spots
- WiFi Hacking
- Hoe kun je veilig werken op locatie?

## 8. DIEV update

### 8.1. Whatsapp fraude

### 8.2. Whatsapp kaping

### 8.3. Deepfake

### 8.4. QR-code fraude

### 8.5. Vacature fraude

### 8.6. Hoe "raadt" een hacker jouw wachtwoord?