

## Interesse in een Human Firewall?

# Hoe herken je de cybercrimineel

**Natuurlijk beschermt u uw bedrijfsgegevens. U zorgt ervoor dat technische maatregelen, zoals antivirus, firewalls, IDS/IPS op orde zijn. Daarom gaan cybercriminelen steeds vaker op zoek naar de zwakste schakel in de beveiliging van uw bedrijfsgegevens: de mens. Uw medewerkers zijn voor opportunistische hackers een gemakkelijk aanvalspunt.**

### DE HUMAN FIREWALL

De online training DIEV™ is in de periode 2018-2021 geleverd aan meer dan 85.000 medewerk(st)ers met als doelstellingen :

- medewerkers kennis/vaardigheden aanleren om Cybercrime te herkennen en tegen te gaan
- jaarprogramma om Security Awareness te kweken, je kunt het niet trainen maar je moet het kweken
- (bijdragen aan) AVG compliancy

Met de online training DIEV™ (Data Informatie Eind-gebruikers Veiligheidstraining) creëert u een extra beveiligingslaag. Wij noemen dat de HUMAN FIREWALL. In de online DIEV™ training leren u en uw medewerkers de acties van cybercriminelen herkennen (zoals phishing, hacking en ransomware e-mails) en datalekken voorkomen. Het aantal beveiligingsrisico's is de afgelopen jaren exponentieel gegroeid. Een belangrijke oorzaak is dat werknemers zich via steeds meer apparaten en toegangspunten aanmelden op het bedrijfsnetwerk. Organisaties worden hierdoor blootgesteld aan grote veiligheidsrisico's. Sinds 2016 is een trend zichtbaar: 'mengerichte' tactieken genieten de absolute voorkeur van cybercriminelen. Waarom? Omdat de mens de zwakste schakel is in de beveiliging van uw gegevens.

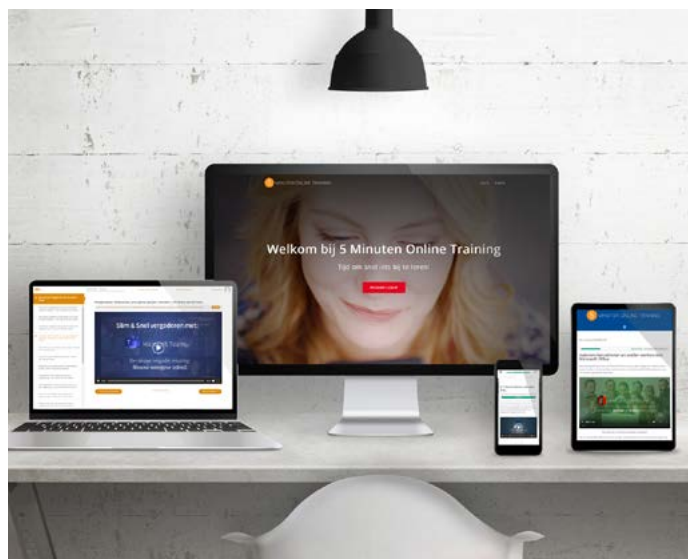
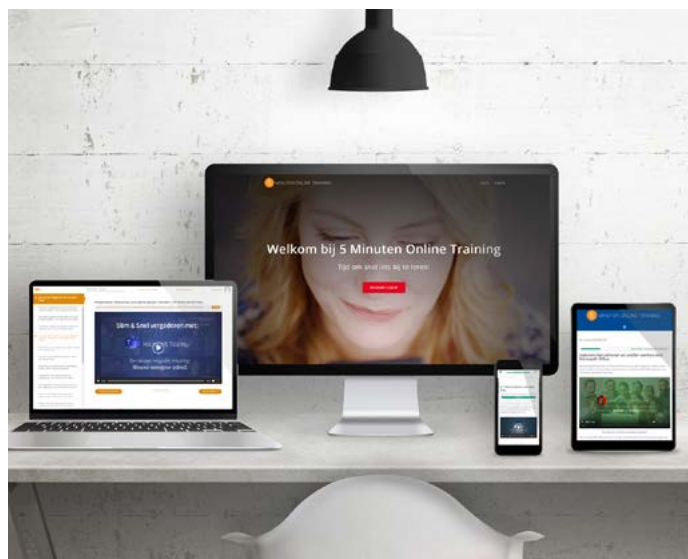
### EEN DATALEK VOORKOMEN

Helaas worden werknemers vaak niet beschouwd als een kernonderdeel van de beveiliging. Dat is een kapitale fout! Juist uw medewerkers vormen voor opportunistische hackers vaak een makkelijk aanvalspunt. In de online training DIEV™, worden u

en uw medewerkers een jaar lang getraind en geïnformeerd. Een gewaarschuwd mens telt voor twee en dit verkleint de kans op datalekken aanzienlijk. Door op tijd de aanval te herkennen wordt verdere schade voorkomen. We maken en houden uw hele organisatie digi-bewust.

### WAT IS HET DOEL VAN DIEV?

DIEV maakt medewerkers bewust van deze risico's en helpt op een praktische manier de risico's te vermijden of er op de juiste manier op te acteren. Met DIEV worden gebruikers getraind in het herkennen van phishing en ransomware e-mails en andere vormen van social engineering. We laten aan de hand van voorbeelden (video's, screenshots, mails e.d.) zien wat de gevaren zijn en dan vooral wat eindgebruikers daar tegen kunnen doen. De basis wordt gevormd door 'bekende' virussen, Ransomware, Phishing, Hacking, ID-fraude, oplichting, gevaren van Free Wifi en Social Media.



## 1. DIEV Introductie

## 2. Vormen van Cybercrime

### 2.0. Introductie

#### 2.1. Phishing

- 2.1.1. Wat is phishing
- 2.1.2. Soorten phishing
- 2.1.3. Phishing herkennen
- 2.1.4. Phishing voorkomen & Wat als je met phishing te maken krijgt

#### 2.2. Virussen

- 2.2.1. Introductie
- 2.2.2. Virussen herkennen
- 2.2.3. Virussen voorkomen

#### 2.3. Internet oplichting

- 2.3.1. Introductie
- 2.3.2. Internet oplichting herkennen en voorkomen

#### 2.4. Hacking

- 2.4.1. Hacking

#### 2.5. Identiteitsfraude

- 2.5.1. Introductie
- 2.5.2. 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 burger service 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 prive 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 smartphone beveiliging
- 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?