



Gehackt!

Eerste hulp bij hacks, phishing, ransomware en andere cybercrime



Eerste hulp bij hacks

Als ondernemer ben je al druk genoeg. Cybersecurity staat daarom niet bovenaan je prioriteitenlijstje. Toch worden 1 op de 3 kleine bedrijven en ondernemers dit jaar getroffen door een vorm van cybercriminaliteit. Voorkomen is beter dan genezen. Maar wat moet je doen als het al te laat is?

Het kan iedereen overkomen

Van een gestolen Instagram account tot een ransomware aanval die je complete bedrijf plat legt. Cybercriminaliteit kent vele vormen met elk zeer ingrijpende gevolgen voor de betrokkenen. Voor een kleine ondernemer kan het al vervelend zijn dat je website of social kanalen volledig plat komen te liggen. Ook is de kans groot dat de daders een flinke smak geld eisen om deze weer terug te krijgen. Wanneer je dit betaalt, is het nog niet zeker of dit ook het geval is. Bij een ransomware aanval zijn de gevolgen vaak nog groter omdat al je systemen en processen stil komen te liggen. Je kunt niet meer bij je data en de daders eisen tienduizenden euro's losgeld. Hoe ga je met dit soort situaties om? In deze gids proberen we advies te geven voor de meest voorkomende situaties.



Phishing EHBO

Bij phishing proberen oplichters persoonlijke gegevens en geld buit te maken. Ze sturen je een mail uit naam van een bekend(e) persoon of organisatie. Wat moet je doen als je de mail hebt geopend en een link hebt aangeklikt?

1. Vul geen gegevens in

Als je alleen op de link in de e-mail hebt geklikt is er nog niet direct een reden voor paniek. Maar vul in elk geval nooit persoonlijke gegevens zoals logins of wachtwoorden in.

2. Sluit de pagina af

Sluit de pagina af. Krijg je ook pop-ups in beeld te zien? Klik niet op de knoppen en sluit deze ook direct af.

3. Run je virusscanner

Zorg dat je virusscanner up to date is en voer een uitgebreide scan uit. Het kan zijn dat er op de achtergrond virussen of malware zijn gedownload. Een virusscan kan deze direct opsporen en verwijderen.

4. Licht je IT-manager in

Wanneer je voor een (groter) bedrijf werkt of in een bedrijfsverzamelgebouw en onderdeel bent van een bedrijfsnetwerk is het belangrijk om je IT-beheerder op de hoogte te stellen van het incident, zodat hij of zij eventueel een uitgebreidere scan van het netwerk en je hardware kan uitvoeren.

5. Toch gegevens ingevuld?

Heb je toch gegevens ingevuld? Dan is het zaak om direct actie te ondernemen. Pas zo snel mogelijk je wachtwoorden aan en neem contact op met de desbetreffende instantie. Run een virusscan en stel je IT-beheerder op de hoogte. En blijf alert op verdachte activiteiten.

6. Doe aangifte

Wanneer je te maken krijgt met diefstal als gevolg van phishing is het belangrijk om hier aangifte van te doen bij de politie: 0800 - 8844



Help, mijn Insta is gejat

Het is menig influencer en bedrijf al eens overkomen: een gehackt Instagram account. Maar ook je e-mail account, WhatsApp, Facebook pagina, TikTok of X-profiel kunnen in de handen van oplichters vallen. Vooral accounts met veel volgers zijn slachtoffer. De hackers eisen vaak losgeld en in ruil voor een betaling krijg jij je social media account weer terug.

Wat moet ik doen?

Veel sociale netwerken bieden oplossingen als je account gehackt is. Zo kun je bij Instagram de app openen op je telefoon. Je ziet dat je niet langer bent ingelogd. Klik in het inlogschermpje op 'Hulp bij aanmelden'. Klik daarna op 'Meer hulp nodig' en volg de instructies. Je ontvangt onder meer een code in je e-mail of via SMS. Zo kun je weer toegang krijgen tot je account.

Als dat niet werkt

Wanneer het niet lukt om via de app weer toegang te krijgen tot je account, kun je nog een oplossing vinden in het [helpcentrum van Instagram](#). Daar vind je een stappenplan waarbij je je identiteit kunt verifiëren.

Hoe kan dit gebeuren?

Hackers hebben waarschijnlijk toegang gekregen tot je account omdat ze je wachtwoord hebben geraden of verkregen uit een datalek. Kies daarom altijd voor unieke wachtwoorden en update deze regelmatig.



Instagram beter beveiligen

Daarnaast is het zinvol om tweefactorauthenticatie aan te zetten op al je social media accounts. Dit kun je vinden onder instellingen. Je moet dan bij een inlogpoging op een nieuw apparaat, altijd een code invullen die via sms- of een app verstuurd wordt. Hackers ontvangen deze code niet en kunnen dan dus ook niet inloggen. Het is een simpele oplossing die veel problemen voorkomt.

Ransomware, wat nu?

Het kan iedereen overkomen: ransomware. Hackers hebben toegang gekregen tot je systemen en ineens gaat je laptopscherm op zwart: 'your files have been encrypted' en er wordt losgeld geëist. Wat moet je doen?

1. Probeer de computer te isoleren

Als één van de computers binnen jouw netwerk is getroffen door ransomware, probeer deze dan direct te isoleren door de internetverbinding te verbreken. Trek niet de stekker eruit, dat helpt niet.



2. Breng iedereen op de hoogte

Het is belangrijk om collega's of een IT-afdeling zo snel mogelijk op de hoogte te stellen van het incident, zodat zij vervolgstappen kunnen nemen.

3. Start het incident response plan

Als je een incident response plan hebt gemaakt, stel deze dan in werking. Ransomware raakt veel verschillende afdelingen en het is zaak dat iedereen weet wat hij of zij moet doen. Heb je geen plan? Het Nationaal Cyber Security Center heeft een Incidentresponsplan Ransomware opgesteld dat je [hier gratis kunt downloaden](#).

4. Zelf oplossen

Je kunt proberen de encrypted bestanden via een ander apparaat te ontsleutelen. Op [Fraudehelpdesk](#) vind je instructies hoe je ransomware kunt verwijderen. De Politie en Europol hebben ook [een tool](#) gemaakt waarmee je sommige ransomware zelf kunt decrypten.

5. Zet back-ups terug

Als je (offline) back-ups hebt van je bestanden, kun je deze terugzetten op een niet geïnfecteerd apparaat. Regelmatig back-ups draaien is daarom heel erg belangrijk.

6. Maak melding

Wanneer je te maken krijgt met ransomware is het belangrijk om hier aangifte van te doen bij de politie: 0800 - 8844. Bij een datalek moet je ook melding doen van het incident bij de [Autoriteit Persoonsgegevens](#) binnen 72 uur.

Maak het ze moeilijk

Juist als je vaak thuis of op locatie werkt loop je meer risico om gehackt te worden. Je bent dan niet beschermd met de veilige firewall en netwerkbeveiliging van kantoor. Maar met deze ijzersterke cybersecurity maatregelen blijf je hackers voor.

1. Gebruik een malwarefilter

Voorkom dat oplichters schadelijke software zoals virussen, spyware of ransomware op jouw laptop kunnen installeren door gebruik te maken van een malwarefilter. Deze maatregel verhindert dat onbetrouwbare software gedownload en geïnstalleerd kan worden. Bij KPN Kleinzakelijk Internet ontvang je standaard een [malwarefilter](#) op je internetverbinding. Het zorgt ervoor dat alle met je modem verbonden apparaten, dus niet alleen laptops maar ook mobieltjes, tablets, slimme deurbellen of wasmachines, beveiligd zijn tegen malware. Je kunt het malwarefilter zelf aan of uit zetten via MijnKPN.

2. Gebruik een wachtwoordmanager

Zorg dat je voor al je (social, e-mail en software) accounts veilige wachtwoorden instelt en dat je deze opslaat in een wachtwoordmanager. Zo'n app onthoudt al je wachtwoorden op één veilige plek. Vaak kun je de app op desktop en mobiel gebruiken, en vult deze zelf de wachtwoorden voor je in als je deze ergens wilt gebruiken. Bij KPN Kleinzakelijk en KPN EEN MKB bieden we voor al onze klanten ook een wachtwoordmanager aan.

3. Zet tweefactorauthenticatie aan

De belangrijkste tip om gehackte social- of e-mail accounts te voorkomen is het aanzetten van 2FA, oftewel tweefactorauthenticatie. Als een hacker bijvoorbeeld probeert in te loggen op je Facebook profiel, ontvang jij direct een sms op je mobiel. Een goed moment om gelijk je wachtwoord weer eens te veranderen.

4. Installeer een virusscanner

Een virusscanner op je laptop is eigenlijk een basismaatregel als je ondernemer bent. Kies bijvoorbeeld voor de [veilige virusscanner van F-Secure](#), wereldwijd marktleider in antivirussoftware. Je kunt F-Secure trouwens heel makkelijk toevoegen aan je Zakelijk Internet abonnement via MijnKPN.

5. Maak back-ups

Vergeet niet om regelmatig (liefst automatisch) back-ups van al je data en bestanden te maken. Kies voor een back-up in de cloud, maar ook voor een fysieke back-up (harddrive) die je bewaart op een andere locatie dan waar je woont of werkt. Besef je dat hackers ook harde schijven en cloudomgevingen kunnen besmetten met ransomware. Zorg dus altijd voor een 'offline' backup.



Veilig je bedrijf laten groeien

Als ondernemer ben je al druk genoeg. Orders aannemen, facturen sturen of je website onderhouden: cybersecurity is vaak niet het eerste waar je aan denkt. Daarom bouwt KPN aan een netwerk en de digitale oplossingen waardoor jij 24/7 beter beschermd bent tegen cyberaanvallen. Voor onze kleinzakelijke en mkb-klanten.

Wil je meer weten wat wij als KPN Zakelijk voor jouw bedrijf kunnen betekenen? Maak dan nu een afspraak met onze ICT-adviseurs:

→ kpn.com/adviesgesprek