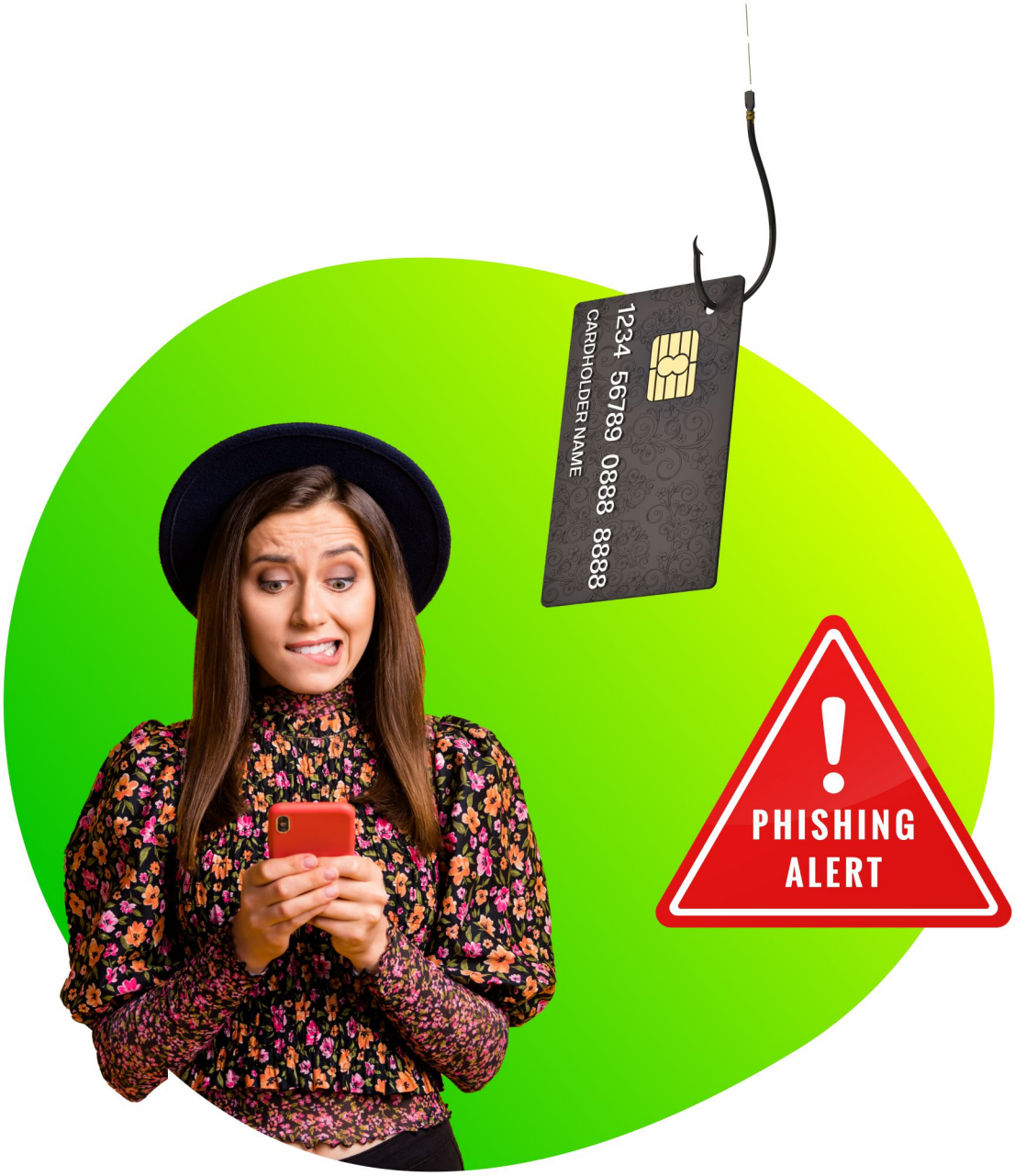


Gehackt!

Eerste hulp bij hacks, phishing, ransomware en andere cybercrime

kpn

Eerste hulp bij hacks
Voor ondernemers en mkb'ers

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 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.

In deze gids lees je..

- Wat je moet doen als je op een phishing link hebt geklikt
- Hoe je moet handelen als je (social) accounts zijn gehackt
- Welke stappen je direct moet zetten als je te maken krijgt met een ransomware aanval

Phishing EHBO

Toch op die foute link geklikt?

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

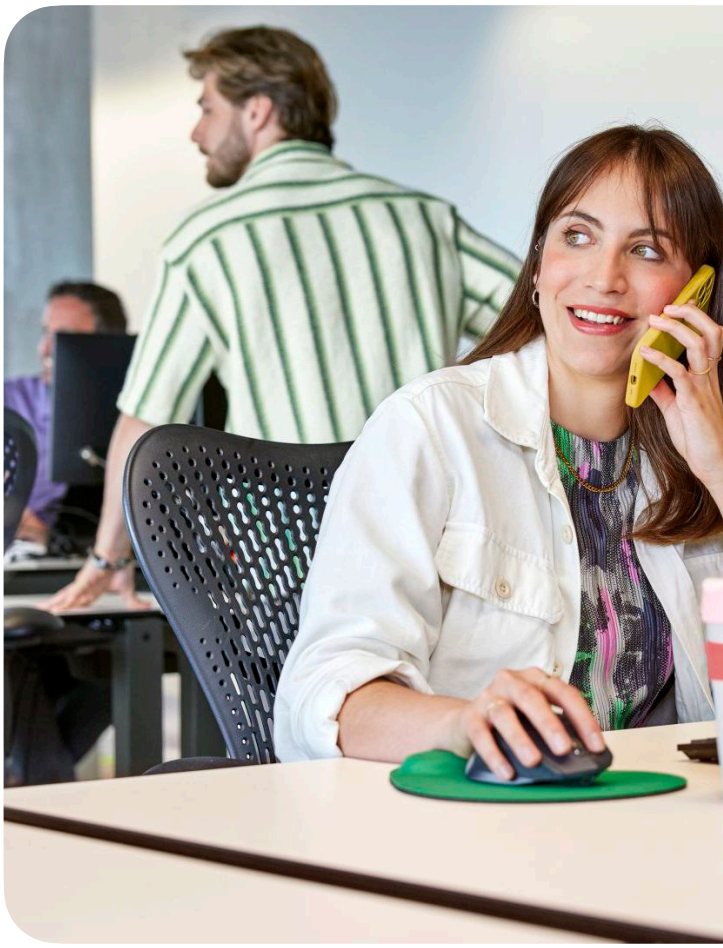
Wanneer je voor een (groter) bedrijf werkt en onderdeel bent van een bedrijfsnetwerk is het belangrijk om je IT-beheerder op de hoogte te stellen van het incident, zodat hij of zij eventueel een uitgebreidere scan van het netwerk en je hardware kan uitvoeren.

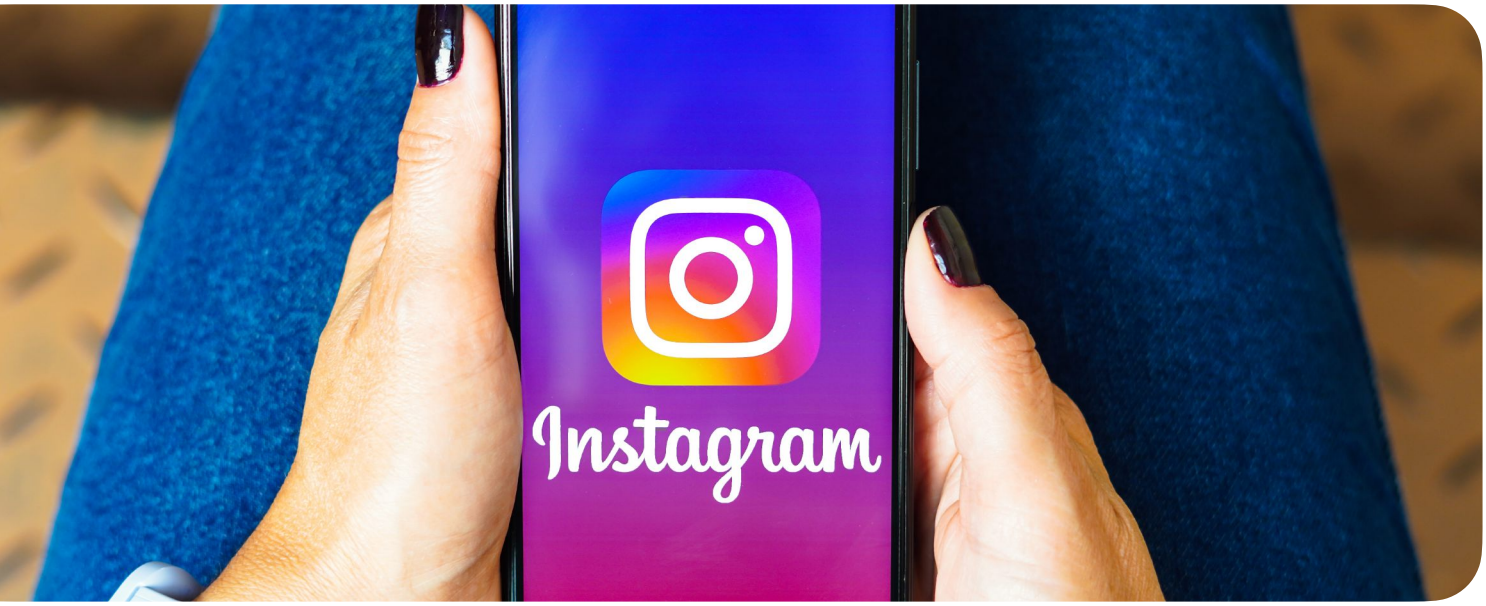
5. Toch gegevens ingevuld?

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





Je account is gehackt

Help, hoe krijg ik mijn Insta terug?

Ik kom niet meer in mijn account

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 cybercriminelen 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 inlogscherm 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, lange en veilige wachtwoorden en update deze regelmatig.

Instagram beter beveiligen

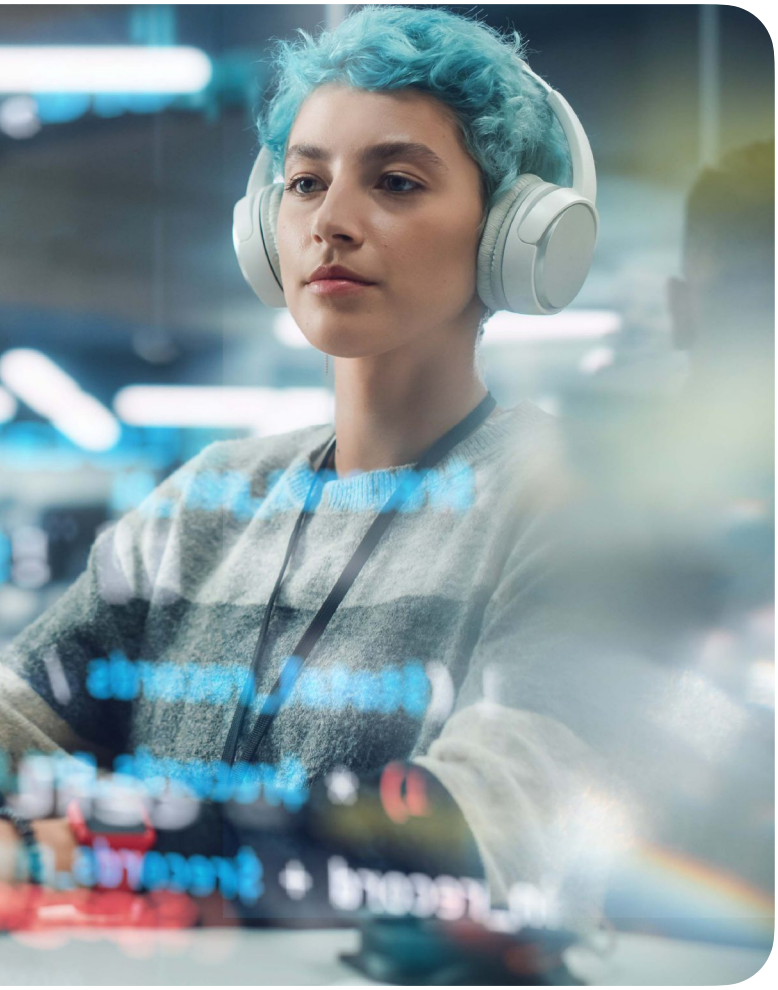
Daarnaast is het zinvol om tweefactorauthenticatie aan te zetten op al je social media accounts. Dit kun je vinden onder instellingen. Je moet dan bij een inlogpoging op een nieuw apparaat, altijd een code invullen die via sms- of een app verstuurd wordt. Hackers ontvangen deze code niet en kunnen dan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

Ransomware aanval
Wat als alles plat ligt

Het kan iedereen overkomen, óók de slager op de hoek. 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 bedrijfsnetwerk is getroffen door ransomware, probeer deze dan direct te isoleren door de internetverbinding te verbreken.

2. Breng betrokkenen 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.

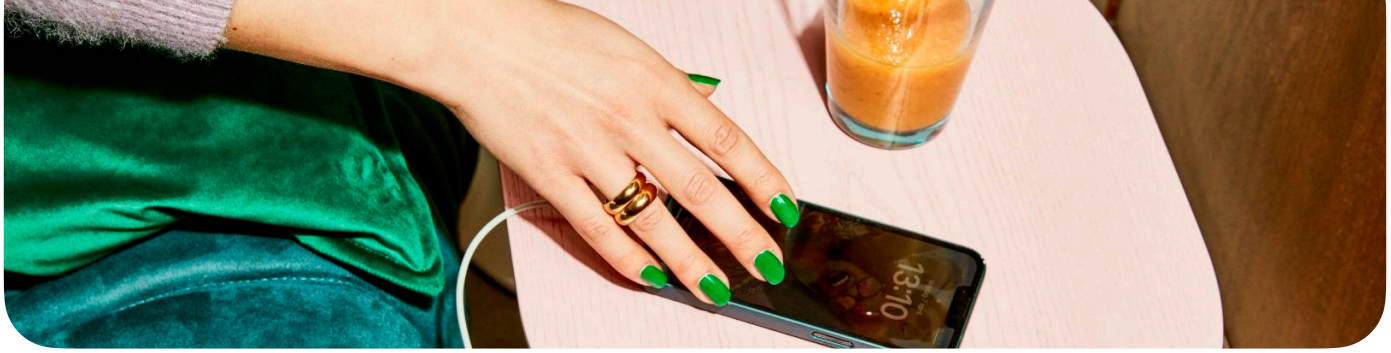


3. Start het incident response plan
Als je bedrijf een incident response plan heeft, stel deze dan in werking. Ransomware raakt veel verschillende afdelingen en het is zaak dat iedereen weet wat hij of zij moet doen. Heb je geen plan? Het Nationaal Cyber Security Center heeft een Incidentresponsplan 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. Back-ups terugzetten
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.



Ransomware voorkomen

Het belang van cyber security

Thuiswerkende collega's zijn een ideaal doelwit voor cybercriminelen. De solide beveiliging van het kantoor ontbreekt vaak in het thuiskantoor. Werknemers werken bijvoorbeeld op een privélaptop zonder beveiliging. Met ijzersterke cybersecurity op alle apparaten en systemen blijf je hackers voor. Hoe beveilig je data en apparaten? Vier tips.

Werk via VPN

Met een Virtual Private Network (VPN) maak je op een veilige manier versleuteld verbinding met het IT-systeem van het werk. Zo werken collega's overal in de beveiligde omgeving van de organisatie. Een VPN neem je af van een VPN-aanbieder. KPN kan je hierover adviseren.

Mobile Device Management

Met Mobile Device Management (MDM) kan je IT- of facilities-afdeling alle hardware binnen je organisatie installeren, beheren en beveiligen vanuit één centraal punt. Hierop regelen zij ook de instellingen, software, gebruikersrechten en het beveiligingsbeleid. Naast het beveiligen van de apparaten, is het beveiligen van data een ander belangrijk punt. Als iets wordt gestolen of kwijtraakt, maar wel goed is vergrendeld, kan de data worden gewist. Zo voorkom je een mogelijk datalek.

Multi Factor Authenticatie

Implementeer op belangrijke systemen 2FA (tweestapsverificatie) of zelfs MFA (multifactorauthenticatie). Na het normale inloggen moet je dan ook nog een code invoeren die je op een ander device, bijvoorbeeld je mobiel, krijgt. Een hacker heeft die niet en komt zo niet door de tweede check. Deze extra beveiliging is in te zetten op bestanden, systemen en apparaten.

Beveilig harde schijven en USB-sticks

Zaken staan veilig op de harde schijf of een usb-stick? Think again. Hackers zijn inmiddels slim genoeg om ook die te kraken. Stel een code in op deze hardware. Mocht je de hardware onverhoopt kwijtraken, is de gevoelige data zodanig versleuteld dat de vinder er niet zomaar bij kan. Tip: zorg dat medewerkers verschillende wachtwoorden gebruiken en laat ze gebruikmaken van een wachtwoordmanager.

Beperkt het risico op cybercriminaliteit met onze **Checklist Cyber Security**

Extra veilig ondernemen van A tot Z met KPN

Met KPN ben jij beter beschermd tegen cyberaanvallen. Dat komt omdat ons internet standaard extra beveiligd is. Voor onze kleinzakelijke en mkb klanten. Daarnaast helpt KPN je ook op weg met het beschermen van je apparaten en data. Kies ook voor extra veilig ondernemen van A tot Z met KPN.

Vraag een vrijblijvend adviesgesprek aan
KPN kan jouw bedrijf helpen bij het zo veilig mogelijk inrichten van je ICT-infrastructuur. Vraag een vrijblijvend adviesgesprek aan om je op maat te laten adviseren:
➜ https://www.kpn.com/advies-op-maat