Bekijk uzelf in cyber

Een kennismaking met de cyberrisico's

CYBEREADY

Laten we beginnen

CYBEREADY

Voor u begint:

Deze oefening is bedoeld om u te helpen de belangrijkste cyberrisico's te **identificeren**, ze te **begrijpen** en tot het minimum te **beperken**

#1

Kenmerk uw **werkdag**

#2

Ontdek uw **risico's**

#3

Ontdek **waargebeurde verhalen**

#4

Leer **wat u moet doen**

Ik ben klaar →

Eerste stap:

Kenmerk **uw werkdag**

Volgende →

Kies een personage waarin u zich herkent:

Ik krijg elke dag tientallen **e-mails**

Ik werk meestal met **klanten**

Ik werk graag op **openbare plaatsen**

Ik verzorg **betalingen**

Kenmerk **uw werkdag** | Ontdek uw **risico's** | Ontdek **waargebeurde verhalen** | Leer **wat u moet doen**

Krijgt u elke dag tientallen e-mails?

Ontdek uw **risico's**

Volgende →

De risico's

Uw intensieve gebruik van e-mail maakt u bijzonder kwetsbaar voor de volgende vormen van fraude:

Phishing

Business-Email-Compromise (BEC) (aanval via zakelijke e-mails)

Wat betekent het? →

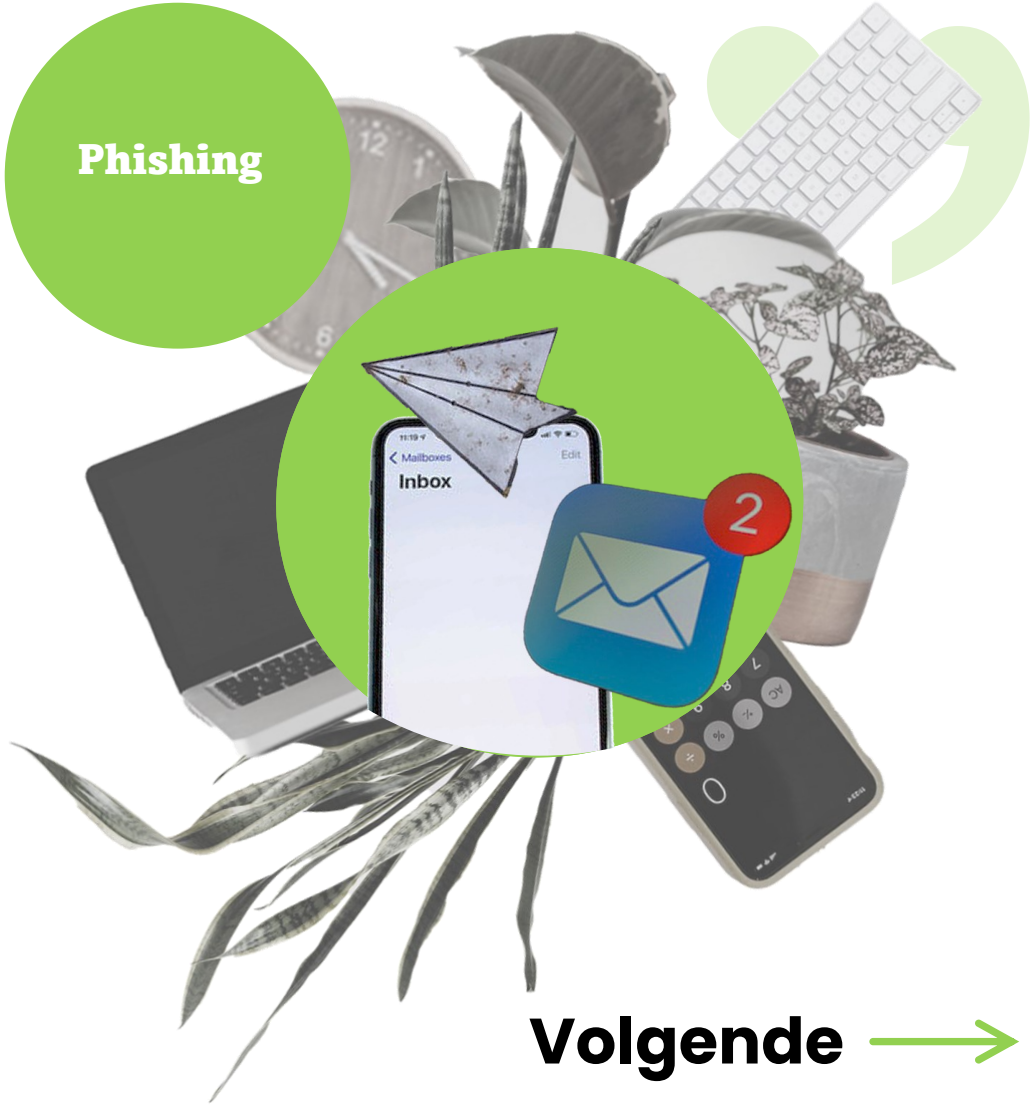
Ontdek waargebeurde verhalen

Elke dag worden mensen het slachtoffer van deze vorm van fraude.
Dit zijn enkele **verhalen** die u zullen helpen om deze risico's te begrijpen

Volgende →

“Het was zo'n dag dat ik niet eens tijd had voor een kop koffie. Ik **kreeg een e-mail** van 'Human Resources'. Hij bevatte een link naar een formulier met vragen over mijn gegevens, zoals mijn e-mail bij het bedrijf en mijn wachtwoord.

Tijdens de lunch **ontdekte ik dat geen enkele collega zo'n formulier had ontvangen**. Was het phishing?”



Volgende

Phishing

"**Ik kreeg een e-mail** van een klant die vroeg om hem te helpen toegang te krijgen tot zijn gegevens. Hij schreef dat hij op het punt stond een contract te tekenen en snel een financieel overzicht nodig had. **En dus deelde ik die vertrouwelijke informatie met hem**.

Toen ik de e-mail later opnieuw bekeek, zag ik **dat het adres niet klopte**. **Zelfs de naam was verkeerd gespeld**."

Volgende →

“**Ik kreeg een e-mail** van 'Daniel Linkens', mijn baas. Hij vroeg om meteen **geld over te schrijven naar een leverancier**, opdat we geen contractbreuk zouden plegen.
Toen ik dat snel had gedaan, vond ik dat ik knap werk had geleverd.

Pas later, toen ik de e-mail opnieuw bekeek, besefte ik dat **er iets heel erg mis was**.”

Volgende →

En nu de laatste stap:

Leer wat u moet doen →

4 tips om uw risico's te beperken

#1 **Controleer** het e-mailadres van de afzender, lijkt het te kloppen?

#2 **Neem contact op met de verzoeker** via een ander kanaal (altijd als het verzoek verdacht lijkt)

#3 **Wijs de link aan** om te verifiëren of de URL naar een gekende site verwijst
(op een mobiele telefoon wordt het adres van de website zichtbaar als u op de link blijft drukken)

#4 **Let op voor e-mail die u vragen om dringend iets te doen.** Dat is een alarmsignaal.

Klaar →

Werkt u meestal met klanten?

Ontdek uw **risico's**

Volgende →

De risico's

Als u met veel mensen werkt (zoals in de klantendienst) bent u bijzonder kwetsbaar voor deze risico's:

Identiteitsfraude

Delen van vertrouwelijke informatie

Wat betekent het? →

Ontdek waargebeurde verhalen

Elke dag worden mensen het slachtoffer van deze vorm van fraude.
Dit zijn enkele **verhalen** die u zullen helpen om deze risico's te begrijpen

Volgende →

“**Ik kreeg een e-mail** van “Ben” van de klantendienst. Hij had documenten nodig voor het project waar ik aan werkte. **Ik stuurde ze hem**.

Pas toen ons bedrijf werd aangeklaagd, **ontdekte ik dat er geen Ben bij de klantendienst was**.”

Volgende →

Delen van vertrouwelijke informatie

"**Mijn baas vroeg om de spreadsheet met onze jaaromzet** naar Michael van Finance sturen, **dat deed ik**. Een week later stond hij in het nieuws.

Ik had de spreadsheet per ongeluk naar een verkeerde Michael in een ander bedrijf van de groep gestuurd."

Volgende →

“**Een vrouw belde me** snikkend op. Haar zoontje van 13 was verdwenen en ze vroeg het log van zijn gesprekken. **Ik wilde haar meteen helpen**, zonder te veel vragen te stellen.

Later ontdekte ik dat **ik de gegevens naar een privédetective** had gestuurd die een geval van overspel onderzocht. Er kwam een proces van.”

Volgende stap

En nu de laatste stap:

Leer wat u moet doen →

4 tips om uw risico's te beperken

#1 **Verifieer altijd** de identiteit van de persoon met wie u mailt

#2 Voor u informatie over klanten deelt, moet u **zeker controleren** dat de informatie mag worden vrijgegeven

#3 Deel gevoelige informatie **uitsluitend via de aangewezen kanalen**

#4 Let op de **toon van de persoon** die u iets vraagt. Als men probeert u onder druk te zetten, is dat meestal een signaal van fraude

Klaar →

Werkt u op openbare plaatsen?

Ontdek uw **risico's**

Volgende →

De risico's

Op openbare plaatsen werken, maakt u bijzonder kwetsbaar voor deze risico's:

Laptopdiefstal

Over uw schouder kijken

Wifi-aanval

Wat betekent het? →

Ontdek waargebeurde verhalen

Elke dag worden mensen het slachtoffer van deze vorm van fraude.
Dit zijn enkele **verhalen** die u zullen helpen om deze risico's te begrijpen

Volgende →

“Het was druk op de **trein**. **Ik werkte op mijn laptop**, want ik moest een belangrijk rapport voltooien. De volgende dag zag ik op Reddit een post met **vertrouwelijke informatie uit mijn rapport**.

Kwam dat **lek** van mij?”

Volgende

Laptopdiefstal

"Ik **werkte in een koffiebar** waar ik vaak kom, **stond even op** om een gebakje te halen en **liet mijn laptop maar heel even achter**.

Toen ik terugkwam, **was hij weg**."

Volgende →

“Ik was op weg naar een klant maar moest nog iets nakijken. **Ik ging dus naar een koffiebar met gratis wifi**, maakte verbinding en vond mijn informatie.

Een maand later **werd mijn identificatie gebruikt om ons systeem te hacken**. Ik vraag me nog altijd af of dat door die gratis wifi komt.”

Volgende stap

En nu de laatste stap:

Leer wat u moet doen →

3 tips om uw risico's te beperken

#1 **Houd uw laptop altijd bij u.** Het zou u verbazen hoeveel laptops elk jaar worden gestolen.

#2 **Gebruik uitsluitend veilige internetverbindingen**, nooit publieke

#3 Zorg dat **alleen u** het scherm van uw laptop en uw notities kunt zien

Klaar →

Verzorgt u betalingen?

Ontdek uw **risico's**

Volgende →

De risico's

Uw machtiging om geld over te schrijven, maakt u bijzonder kwetsbaar voor de volgende vormen van fraude:

Business-Email-Compromise (BEC) (aanval via zakelijke e-mails)

Identiteitsfraude van leveranciers

Wat betekent het? →

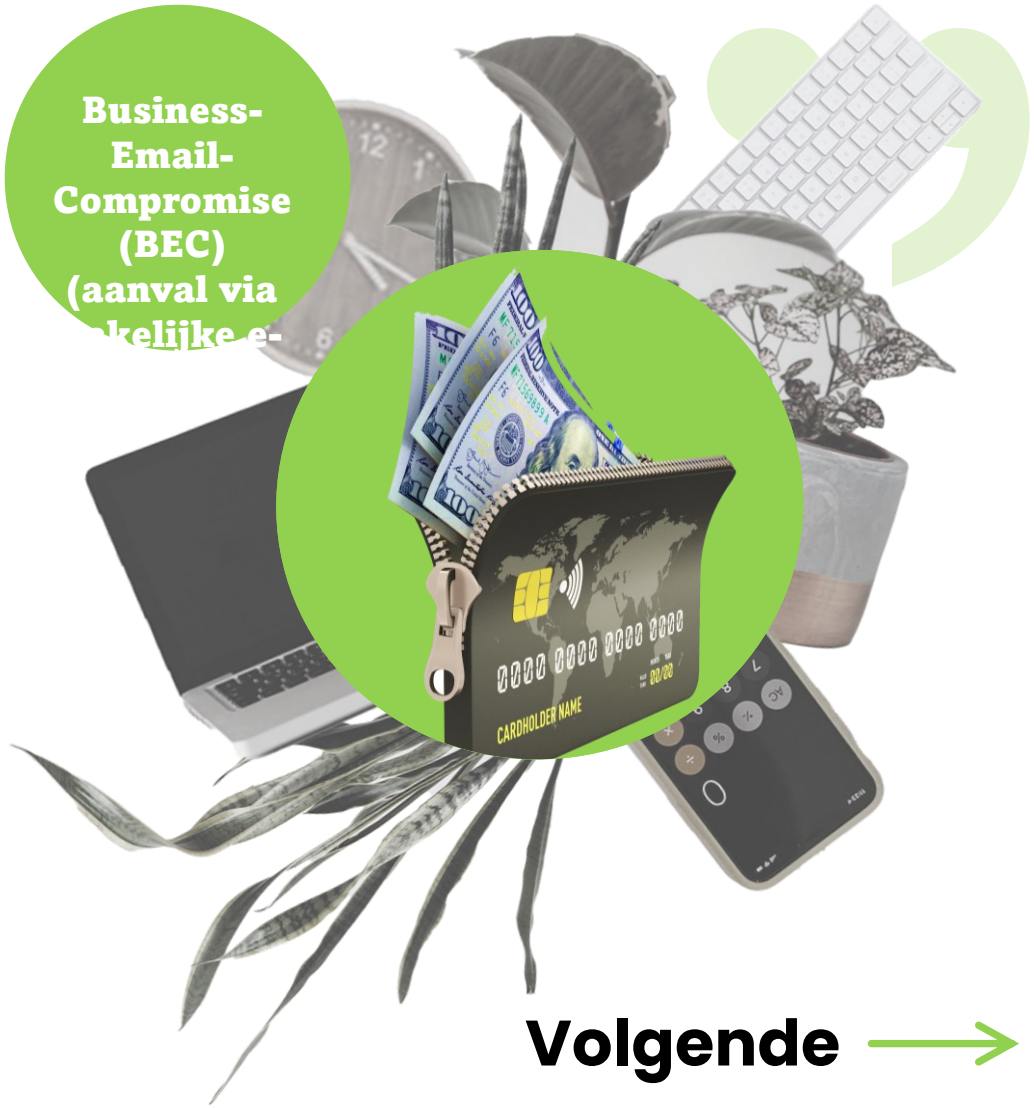
Ontdek waargebeurde verhalen

Elke dag worden mensen het slachtoffer van deze vorm van fraude.
Dit zijn enkele **verhalen** die u zullen helpen om deze risico's te begrijpen

Volgende →

“**Ik kreeg een e-mail** van mijn baas met **de opdracht 17.000 euro aan een nieuwe leverancier te betalen**. “Hij schreef: 'Ben in vergadering, kan niet praten. **Schrijf het bedrag ASAP over**', en dus deed ik dat.”

Maar de volgende dag, op kantoor, besefte ik dat **hij niet wist waar ik het over had**.”



Volgende →

Identiteitsfraude van leveranciers

"**Ik kreeg een e-mail** van de **nieuwe financieel directeur** van een van onze leveranciers, met de vraag om de **betalingen voortaan** naar een andere bankrekening over te schrijven." **Dat deed ik dus**.

Het was **fraude**, maar hoe kon ik dat weten?"

Volgende →

“**Ik kreeg een e-mail** van HR met een lange lijst van namen. Ze vroegen om **geschenkbonnen** voor het nieuwjaarsfeest te kopen. En of ik de nummer van de bonnen wou doorsturen. **Ik kocht de bonnen en stuurde hen de nummers**.

Later bleek het fraude te zijn en was **al het geld weg**.”

Volgende stap

En nu de laatste stap:

Leer wat u moet doen →

3 tips om uw risico's te beperken

#1 **Controleer** het e-mailadres van de afzender. Als het niet het normale adres is, moet u de e-mail sluiten en op een andere manier contact opnemen met de vermeende afzender

#2 **Verifieer elk verzoek** om een betaalmethode te wijzigen met uw normale contactpersoon, persoonlijk of telefonisch.

#3 **Haast u niet.** Hackers proberen mensen op te jagen, zodat ze alarmsignalen niet zien en niet met anderen overleggen

Klaar →

Knap! U hebt de oefening voltooid

Wat wilt u nu doen?

Een andere oefening verkennen **Voltooien**

Dank u voor uw medewerking

Wij hopen dat u het interessant vond en kostbare inzichten hebt verworven