

Vraag 1/10

Iemand die ik niet ken, vraagt me om een foto van mijn bankkaart door te sturen, zodat hij een bedrag aan mij kan overmaken. Wat doe ik?

Geen probleem, met een foto alleen kan hij niks doen, toch?

No way, met de gegevens op mijn kaart kan hij online betalingen doen.

Ik doe het niet. Wie weet gebruiken ze de gegevens op de kaart ooit om mij een vals gevoel van vertrouwen te geven.

Vraag 2/10

Zodra ik merk dat ik het slachtoffer ben van phishing, moet ik zeker 3 instanties contacteren: de politie, Card Stop en ...

De federale overheidsdienst financiën zodat die al mijn geldstromen kunnen traceren.

Je bank zodat ze mijn betaalrekening kunnen blokkeren zodat phishers geen transacties meer kunnen uitvoeren.

De phishers zelf, zodat ik hen eens goed de les kan spellen.

Vraag 3/10

Ik krijg een mail van een vriend waarin een interessante link zit. Wat doe ik?

Ik klik meteen op die link. Ik ken die vriend, alles wat hij mij mailt is te vertrouwen

Ik bel die vriend om te vragen of hij mij wel degelijk zo'n mail heeft gestuurd en of die link te vertrouwen is.

Ik vertrouw het misschien niet helemaal maar klik toch op de link, want gewoon doorklikken kan geen kwaad.

Vraag 4/10

Ik krijg een verdachte mail. Die komt van phishers, dat weet ik zeker. Wat doe ik?

Ik stuur de mail naar verdacht@safeonweb.be

Ik ga die phishers eens goed te grazen nemen. Ik speel het spelletje mee en doe wat ze vragen.

Ik stuur de mail door naar al mijn vrienden.

Vraag 5/10

Mijn bank belt me. Ze hebben een verdachte transactie gezien op mijn rekeningen. Wat doe ik?

Ik geef ze alle informatie die ze nodig hebben.

Ik controleer het nummer waarmee ze bellen, is het een betrouwbaar nummer, dan geef ik ze alle informatie die ze nodig hebben.

Ik vertrouw het niet: ik haak in en bel mijn bank zelf om te vragen of zij het echt waren.

Vraag 6/10

Oei, ik heb oplichters toegang gegeven tot mijn bankgegevens! Ik moet onmiddellijk contact opnemen met Cardstop, want zij kunnen:

mijn bankrekening en bankapplicaties blokkeren.

mijn bankkaarten en kredietkaarten blokkeren.

zowel mijn rekeningen als mijn bankapplicaties als kaarten blokkeren.

Vraag 7/10

Ik krijg op straat de vraag of ik wat geld wil bijverdienen. Het enige wat ik moet doen is een som geld op mijn rekening laten toekomen en het nadien overschrijven naar een andere rekening. Wat doe ik?

Ik ga er op in. Tenslotte doe je niks mis door gewoon wat geld over te schrijven.

Ik ga er op in. Als ik alleen mijn rekeningnummer geef en geen codes of paswoorden, kan er me niks gebeuren.

Ik zeg nee want ik vertrouw de zaak niet. Als het om crimineel geld gaat, riskeer ik een gevangenisstraf.

Vraag 8/10

Ben je slachtoffer van online oplichting, dan moet je altijd klacht indienen bij de politie?

Klopt, maar er is geen tijdsdruk. Het geld is toch al weg

Klopt, en hoe sneller hoe beter. Als je binnen 48 uur gaat, kan de politie in veel gevallen nog geld traceren en recupereren

Klopt niet, de politie kan niks doen dus klacht indienen heeft geen zin

Vraag 9/10

Als je een WhatsAppbericht krijgt van een nieuw nummer met een foto en naam van een bekende, dan mag je het vertrouwen?

Oplichters kunnen geen foto's veranderen op WhatsApp dus je mag het vertrouwen

Als je de naam en foto herkent, dan mag je er zeker van zijn dat het om de echte persoon gaat

Nee, oplichters stelen ook foto's en persoonsgegevens om betrouwbaarder over te komen

Vraag 10/10

Wanneer ik telefoon krijg van de bank en het nummer correct is, kan ik 100% zeker zijn dat het een echte bankmedewerker is die mij belt?

Fout, ook telefoonnummers kunnen nagebootst worden

Klopt, de bank heeft een nummer dat niet nagebootst kan worden

Klopt, telefoonnummers kan je niet nabootsen

Zo, dat waren onze zeven phishing-vragen!

Jij behaalde 10 op 10.

Iemand die ik niet ken, vraagt me om een foto van mijn bankkaart door te sturen, zodat hij een bedrag aan mij kan overmaken. Wat doe ik?

Ik doe het niet. Wie weet gebruiken ze de gegevens op de kaart ooit om mij een vals gevoel van vertrouwen te geven.



JUIST

Je geeft onbekenden beter zo weinig mogelijk persoonlijke informatie, zelfs als die op het eerste gezicht onschuldig lijkt. Oplichters weten vaak meer over je dan je zou denken en die informatie wordt online ook gretig verhandeld. Vooral informatie over nummerplaten of bankrekeningnummers is waardevol, omdat phishers daarmee veel vertrouwen kunnen opwekken bij hun slachtoffers.

Zodra ik merk dat ik het slachtoffer ben van phishing, moet ik zeker 3 instanties contacteren: de politie, Card Stop en ...

Je bank zodat ze mijn betaalrekening kunnen blokkeren zodat phishers geen transacties meer kunnen uitvoeren.



JUIST

Card Stop kan enkel jouw betaalkaarten blokkeren en eventuele betaalapps die eraan verbonden zijn. Maar als phishers toegang hebben tot je online bankomgeving, kunnen ze van daaruit geld overmaken naar een andere rekening. Ze kunnen zelfs je spaarrekening plunderen. Bel daarom ook altijd naar je bank om je rekeningen te laten blokkeren. Alle banken hebben een fraudelijn die 24/7 bereikbaar is. Het nummer vind je op de website van Card Stop.

Ik krijg een mail van een vriend waarin een interessante link zit. Wat doe ik?

Ik bel die vriend om te vragen of hij mij wel degelijk zo'n mail heeft gestuurd en of die link te vertrouwen is.



JUIST

Zie je het e-mailadres van je vriend staan als afzender? Dan nog ben je niet zeker dat de mail wel echt van hem afkomstig is. Phishers slagen er namelijk in om hun mailadres te vermommen als dat van iemand anders. Laat het pijltje van je muis daarom eens zweven boven het emailadres (niet klikken). In heel wat mailprogramma's komt dan het échte mailadres tevoorschijn. Klik zo weinig mogelijk door via links in berichten. Gebruik de link uit je favorieten of typ het adres van de website eigenhandig in de adresbalk bovenaan.

Ik krijg een verdachte mail. Die komt van phishers, dat weet ik zeker. Wat doe ik?

Ik stuur de mail naar verdacht@safeonweb.be



JUIST

Safe On Web verwerkt automatisch duizenden verdachte e-mails per dag. De dienst filtert er de frauduleuze boodschappen uit, zodat de verzenders ervan geïdentificeerd en aangepakt kunnen worden. Stuur dus steevast elke verdachte mail die je krijgt door naar verdacht@safeonweb.be. Je kunt ook een screenshot van een verdachte sms doormailen.

Mijn bank belt me. Ze hebben een verdachte transactie gezien op mijn rekeningen. Wat doe ik?

Ik vertrouw het niet: ik haak in en bel mijn bank zelf om te vragen of zij het echt waren.



JUIST

Let op, banken bellen wel klanten als er verdachte transacties zijn. Maar ze zullen je daarbij nooit om persoonlijke codes vragen of ze zullen je ook nooit vragen om door te klikken op een link die ze jou sturen. Vanaf de eerste twijfel, haak je gewoon in en probeer je zelf te bellen naar je bank. Of je logt zelf in bij je bank via de gewone weg. Dan kan je zelf checken of er inderdaad iets mis is, want de kans is groot dat er dan iets aan de hand is. Want oplichters bellen hun slachtoffers vaak, nadat ze zijn binnengeraakt in jouw account, in de hoop zo nog meer geld te kunnen stelen.

Oei, ik heb oplichters toegang gegeven tot mijn bankgegevens! Ik moet onmiddellijk contact opnemen met Cardstop, want zij kunnen:

mijn bankkaarten en kredietkaarten blokkeren.



JUIST

Card Stop blokkeert voor jou je credit cards, de betaalkaarten die gekoppeld zijn aan je rekeningen en de eventuele betaalapps die aan die kaarten gelinkt zijn, zoals bijvoorbeeld Payconiq. Card Stop blokkeert niet de rekeningen zelf, daarvoor moet je zeker ook contact opnemen met je bank.

Ik krijg op straat de vraag of ik wat geld wil bijverdienen. Het enige wat ik moet doen is een som geld op mijn rekening laten toekomen en het nadien overschrijven naar een andere rekening. Wat doe ik?

Ik zeg nee want ik vertrouw de zaak niet. Als het om crimineel geld gaat, riskeer ik een gevangenisstraf.



JUIST

De zogenaamde 'geldezels' zijn vaak jongeren of kwetsbare mensen die hun rekening ter beschikking stellen om het gestolen geld op te parkeren, tot de daders het afhalen of er aankopen mee doen. Geldezels zijn de onderste laag in de piramide, maar zijn wel medeplichtig aan een crimineel feit en dus ook strafbaar. In Antwerpen loopt het pilootproject 'Mule Stop', waarmee banken sneller kunnen achterhalen waar gestolen geld naartoe versluisd wordt. Het systeem wordt dit najaar in het hele land van kracht.

Ben je slachtoffer van online oplichting, dan moet je altijd klacht indienen bij de politie?
Klopt, en hoe sneller hoe beter. Als je binnen 48 uur gaat, kan de politie in veel gevallen nog geld traceren en recupereren

i
Hoe sneller de politie op de hoogte is van online oplichting, hoe sneller ze actie kunnen ondernemen om gestolen geld te blokkeren. Het heeft dus zeker zin om klacht in te dienen. Daarnaast is het ook belangrijk om klacht in te dienen zodat de politie een duidelijk zicht krijgt op hoe groot het probleem van online oplichting is en welke soorten cybercrime er bestaan.

Als je een WhatsAppbericht krijgt van een nieuw nummer met een foto en naam van een bekende, dan mag je het vertrouwen?

Nee, oplichters stelen ook foto's en persoonsgegevens om betrouwbaarder over te komen

Wanneer ik telefoon krijg van de bank en het nummer correct is, kan ik 100% zeker zijn dat het een echte bankmedewerker is die mij belt?

Fout, ook telefoonnummers kunnen nagebootst worden

i
Er is online software te vinden waarmee je elk oproepnummer kan nabootsen. Criminelen maken daar gebruik van om hun oproepen betrouwbaarder te laten overkomen. Krijg je telefoon van het nummer van de bank, wees dan alert. Als ze om codes of persoonlijke info vragen bel je best zelf terug naar het nummer van jouw bank.