Hou je smartphone veilig

1. Stel de toegangscode van je toestel in met minstens 6 cijfers, gebruik de vingerafdruk of gezichtsherkenning. Op die manier kan iemand die jouw smartphone vindt of steelt niet zomaar aan je gegevens.

2. Zorg dat je smartphone en apps steeds up-to-date zijn. Krijg je de vraag om updates uit te voeren? Doe het zo snel mogelijk. Zet je smartphone regelmatig eens uit. Bij het opnieuw opstarten gebeuren sommige updates automatisch.

3. Download enkel apps uit officiële app winkels: de App Store als je een iPhone gebruikt, de Google Play Store als je een ander merk toestel gebruikt.

4. Kijk uit voor valse sms'jes of WhatsApp berichten. Ze lijken van een bedrijf of een openbare dienst te komen (bank, Itsme®, pensioendienst,...) of beloven je een premie, en ze moedigen je aan om op de links te klikken die ze bevatten om je bankcodes te krijgen en je rekeningen leeg te halen. Wees altijd op je hoede als je een berichtje krijgt van een nummer dat je niet kent.

5. Gebruik een virusscanner op je toestel.

Hou je computer of laptop veilig

1. Leer verdachte berichten herkennen. Veel e-mails die je krijgt, zijn pogingen tot oplichting. Denk altijd 2 keer na als je een bericht krijgt van een onbekende en klik nooit op een link in een verdacht bericht.

2. Installeer een virusscanner op je computer.

3. Voer regelmatig updates uit, zowel voor je besturingssysteem als voor je programma's.

4. Bescherm je computer en je accounts (bv. e-mail, Facebook, …) met een lang wachtwoord van minstens 13 karakters. Gebruik verschillende wachtwoorden.

5. Ken je tweestapsverificatie (2FA) al? Het is niet moeilijk en super veilig. Je beschermt je belangrijke accounts met een dubbel slot. Naast een wachtwoord, gebruik je nog een 2de sleutel, bv. een code die je wordt toegestuurd via sms.

Laat je niet vangen aan de telefoon

1. Krijg je een oproep van een nummer dat je niet herkent? Wees dan altijd op je hoede.

2. Geef nooit persoonlijke gegevens, wachtwoorden, codes van je bankkaart of response codes door tijdens een telefoongesprek.

3. Bel nooit terug naar onbekende nummers. Beantwoord nooit oproepen van buitenlandse nummers die je niet kent. Bel deze nummers zeker niet terug. Als iemand je nodig heeft, zal die wel een boodschap achter laten.

4. Geloof niet zomaar wat men je aan de telefoon vertelt. Microsoft of een ander technologiebedrijf zal je nooit bellen. Je bank vraagt nooit via de telefoon naar je codes of om een nieuwe rekening te openen.

5. Sla de nummers van mensen die je kent op. Blokkeer nummers van ongewenste bellers.

Wat kan je nog meer doen?

Checklist

✓Ik geef nooit persoonlijke gegevens, wachtwoorden, codes van mijn bankkaart of response codes door via een e-mail, telefoongesprek, sms'je, of sociale media.

✓Ik download de Safeonweb app om waarschuwingen te ontvangen over nieuwe vormen van online oplichting en ik volg de tips van de website safeonweb.be.

✓Ik stel een toegangscode in op mijn smartphone.

✓Ik stel 'automatische updates' in op mijn smartphone en computer.

✓Ik installeer een virusscanner op mijn smartphone en op mijn computer, als ik die nog niet zou hebben.

✓Ik sla de nummers van vrienden en familie op in mijn smartphone. Ook de nummers van mijn bank en andere handelszaken die ik vaak nodig heb of die mij mogen contacteren, sla ik op.

✓Ik bescherm mijn e-mailbox met tweestapsverificatie (2FA).

✓Ik bescherm mijn andere accounts (Facebook, Instagram…) met tweestapsverificatie (2FA), waar dit mogelijk is.

VU: Miguel De Bruycker, Wetstraat 18, 1000 Brussel

Vraag hulp!

Weet je niet goed waar te beginnen met deze tips? Twijfel je over een bericht? Merk je 'iets raars' aan je computer? Blijf niet met je twijfel zitten!
Vraag hulp aan vrienden of familie met wat meer ervaring.

Meer info nodig?
Neem een kijkje op www.safeonweb.be en in onze brochure 'Cyberaanvallen en online oplichting'. Download onze Safeonweb-app om op de hoogte te blijven van de nieuwste bedreigingen.

Safeonweb

Heb je een verdachte e-mail of een verdacht bericht ontvangen ?

Stuur het door naar verdacht@safeonweb.be en verwijder het daarna. Je krijgt geen persoonlijk antwoord. De links in het bericht worden geblokkeerd waardoor minder oplettende internetgebruikers geen slachtoffer kunnen worden.

Meldpunt

Ben je slachtoffer van misleiding, bedrog, fraude, oplichting?

Doe dan een melding via meldpunt.belgie.be van de FOD Economie. Je krijgt steeds een advies op het einde van je melding. De bevoegde diensten analyseren de melding en stellen mogelijk een onderzoek in.

Het Centrum voor Cybersecurity België

Safeonweb is een initiatief van het Centrum voor Cybersecurity België.

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

.be

Oplichters te slim af zijn?

3 x 5 tips om jezelf te beschermen

Safeonweb.be