Leer valse mails herkennen

Stuur verdachte berichten naar verdacht@safeonweb.be

Phishing is online oplichting door valse e-mails, websites of berichten. Maar hoe herken je die valse e-mails en hoe maak je het onderscheid met betrouwbare berichten? Slimme cybercriminelen kunnen je echt doen twijfelen. Je vindt hier een aantal tips om te beoordelen of je een bericht kan vertrouwen.

De basisregel

Cybercriminelen proberen altijd om misbruik te maken van iets waar je in gelooft of van iemand die je vertrouwt. Ze proberen ook vaak in te spelen op angst. Laat je niet vangen!

Tips

Vind je een mail of telefoontje verdacht? Beantwoord dan deze vragen:

- **Is het onverwacht?**

Krijg je zonder reden een bericht van deze afzender: je kocht niets, had lang geen contact, enz. Controleer zeker verder.

- **Is het dringend?**

Hou je hoofd koel: kreeg je echt een eerste aanmaning tot betaling? Ken je die 'vriend in nood' wel?

- **Ken je de afzender?**

Controleer het e-mailadres, ook op spellingsfouten. Maar let op: een legitiem e-mailadres is geen garantie.

- **Vind je de vraag vreemd?**

Een officiële instantie zal je nooit via e-mail, sms of telefoon vragen om je wachtwoord, bankgegevens of persoonlijke gegevens.

- **Naar waar leidt de link waar je moet op klikken?**

Zweef met je muis over de link. Is de domeinnaam, het woord voor .be, .com, .eu, .org, … en voor de allereerste slash "/", ook echt de naam van de organisatie?

Een voorbeeld:

- Bij de link www.safeonweb.be/tips is het domein safeonweb.
- Bij de link www.safeonweb.tips.be/safeonweb is 'tips' het domein en word je naar een andere website geleid.

- **Word je persoonlijk aangesproken?**

Berichten met algemene en vage aanspreektitels, of je e-mailadres als aanspreking, die wantrouw je beter.

- **Bevat het bericht veel taalfouten?**

Ook al zorgen doorgewinterde cybercriminelen voor correcte taal, taalfouten of een vreemde taal kunnen wijzen op een verdacht bericht.

- **Zit het bericht in je Spam/Junk folder?**

Indien ja, wees extra voorzichtig. Je kan ook zelf verdachte berichten markeren als Spam of Junk en zo anderen waarschuwen.

- **Probeert iemand je nieuwsgierig te maken?**

Iedereen zou nieuwsgierig worden bij berichten met een link als "Kijk wat ik over jou las ..." of "Ben jij dit op deze foto?", maar laat je niet vangen.

Wat als je twijfelt?

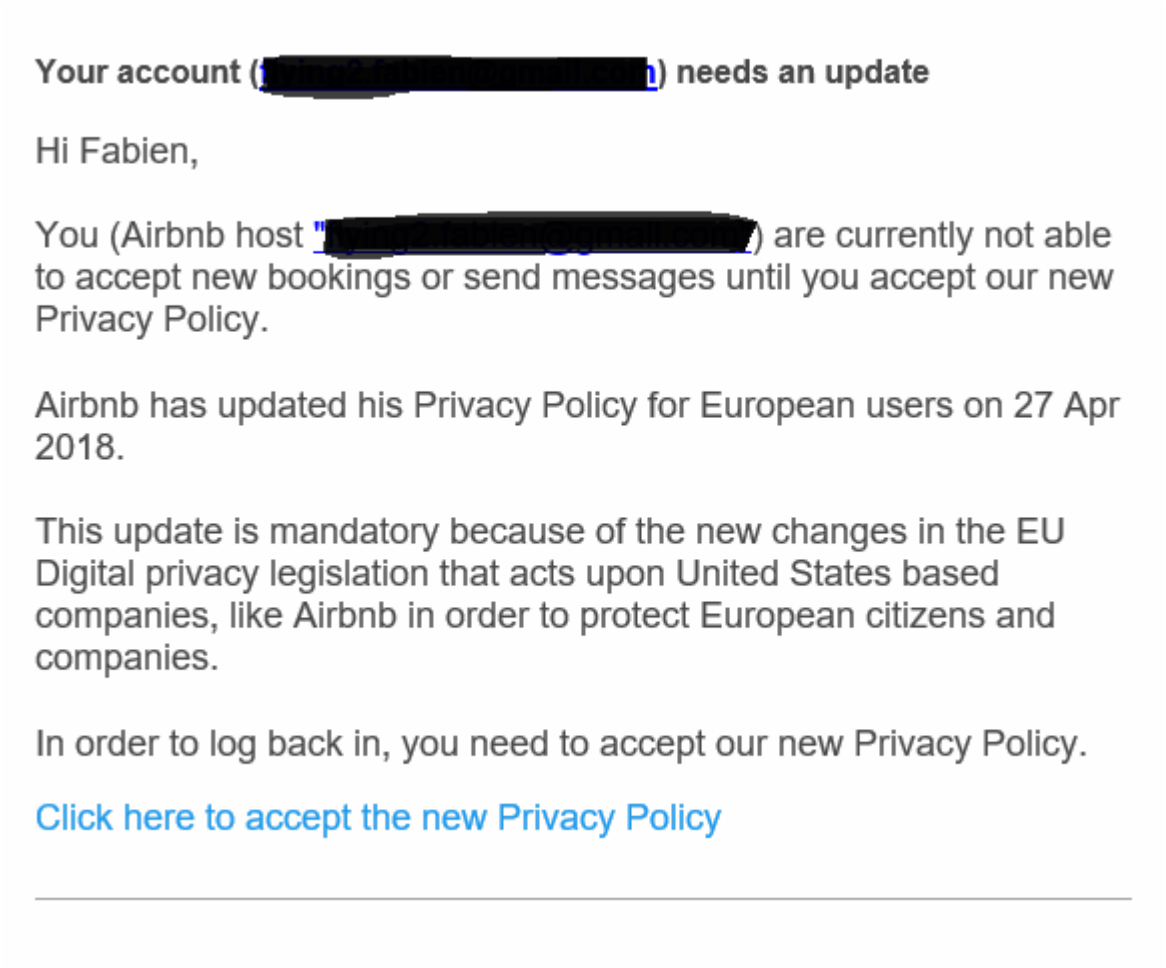
Het is beter om op je hoede te zijn. Als je twijfelt, open dan zeker geen links of bijlagen en neem contact op met de afzender op een andere manier:

- **Vrienden** kan je bellen, sms'en of een bericht sturen via sociale media. Komt het bericht niet van hen, laat dan zeker weten dat hun account gehackt is. Bij sommige sociale netwerken kan je berichten als 'vals' markeren.
- Bij **organisaties** of **bedrijven** ga je naar hun site en controleer je of die 'dringende' actie bestaat. Vind je niets terug, dan kan je ook even bellen.

Ontdek of jij je laat vangen door cybercriminelen met onze phishingtest. Niet alleen leer je er hoe goed jij internetfraude kan herkennen; we wapenen je ook met nog meer praktische tips zodat je niet meer in een phishingval trapt.

Herken jij valse e-mails? Doe de test! VIA DEZE SITE :
https://www.safeonweb.be/nl/quiz/phishingtest

VOORBEELD VALSE MAIL



Your account ([redacted]) needs an update

Hi Fabien,

You (Airbnb host "[redacted]") are currently not able to accept new bookings or send messages until you accept our new Privacy Policy.

Airbnb has updated his Privacy Policy for European users on 27 Apr 2018.

This update is mandatory because of the new changes in the EU Digital privacy legislation that acts upon United States based companies, like Airbnb in order to protect European citizens and companies.

In order to log back in, you need to accept our new Privacy Policy.

Click here to accept the new Privacy Policy

Wat doen als je een vals bericht krijgt?

- **Stuur het door naar verdacht@safeonweb.be**
- Klik niet op de links, maar zoek de website op via een zoekmachine.
- Stuur het bericht niet door naar je contacten.
- Vul zeker nooit persoonlijke gegevens in.
- Je kan het ook doorsturen naar de organisatie zelf.

Te laat! Je hebt je gegevens wel doorgegeven?

- Waarschuw je vrienden dat je hen een vals bericht hebt doorgestuurd.
- Als je een wachtwoord hebt doorgegeven, dat je ook op andere plaatsen gebruikt, verander het dan onmiddellijk.
- Als je je creditcardgegevens hebt doorgegeven, verwittig je onmiddellijk Card Stop op 078 170 170 (+32 78 170 170 uit het buitenland).