Politie

Federal Computer Crime Unit

Internetfraude

Sinds de komst van het internet hebben oplichters nieuwe manieren gevonden om op een makkelijke en snelle manier veel mensen geld afhandig te maken. Vandaag de dag communiceert een groot deel van de bevolking via e-mail en heeft men thuis of op het werk toegang tot het internet. De kans dat je op de een of andere dag geconfronteerd wordt met personen die je via deze weg proberen op te lichten is dan ook zeer reëel. Wees daarom steeds alert wanneer je benaderd wordt door ***ONBEKENDEN*** via het internet.

Tegenwoordig is het moeilijk om te ontkomen aan de veelheid aan ***SPAM*** die wordt verstuurd naar onze mailboxen. Tussen al deze ongewenste reclameboodschappen van personen en bedrijven waar men nog nooit van gehoord heeft, zitten vaak mails - in het Engels of in slecht Frans of Nederlands geschreven - die als onderwerp neploterijen, de nalatenschap van een Afrikaans staatshoofd, hulp bij geldtransacties, exotische investeringen, of dergelijke meer hebben.

Oplichters zijn erg creatief en zoeken steeds nieuwe manieren om mensen geld af te troggelen. Toch zien we steeds dezelfde basisvormen terugkomen; hieronder vind je enkele van de meest voorkomende. De beste raad: ***DEZE MAILS NEGEREN EN ZE METEEN WISSEN***! Ga er vooral nooit op in, je riskeert veel geld kwijt te raken!

Zo win je bijvoorbeeld plots enkele miljoenen dollars of euro's, en dat terwijl je nooit hebt deelgenomen aan enige ***LOTERIJ***! Om het geld te ontvangen moet je wel eerst allerlei kosten betalen: administratiekosten, notariskosten, bankkosten, etc. Of één van de weduwes van wijlen een Afrikaans staatshoofd schrijft je persoonlijk aan – wat een eer! - met de vraag haar te helpen om de ***ERFENIS*** die ze kreeg van haar man uit het land te sluizen. Het enige dat je moet doen is gewoon enkele bedragen voorschieten, en nadien zul je gegarandeerd een percentage krijgen van het totale bedrag, dat uiteraard in de miljoenen beloopt.

Er bestaan vele varianten van deze vorm van oplichting, maar het basisprincipe blijft hetzelfde: je moet geld voorschieten aan een onbekende om een beloofde som geld binnen te rijven. Vaak maken de oplichters gebruik van echt uitziende documenten (van notarissen, banken, paspoorten, enz.) die ze via mail doorsturen. Ook deze zijn vervalst!

Veel voorkomend zijn ook de mails waarin je ***BANK*** je zogenaamd contacteert omdat er problemen zijn met het internetbankingsysteem, of omdat je gegevens dienen aangepast te worden. Daarvoor moet je op een link in de mail klikken, en die lijkt je op een pagina van de bank te brengen waar men je vraagt om je logingegevens en paswoord in te geven, en soms nog meer persoonlijke gegevens als adres, telefoonnummer en geboortedatum ("*phishing*"). Doe dit vooral niet! Oplichters proberen op deze manier je persoonlijke gegevens te stelen om ze nadien te misbruiken. Denk eraan dat je bank je ***NOOIT*** via mail zal contacteren om je persoonlijke gegevens op te vragen!

Ook oplichtingen via ***ZOEKERTJESSITES*** als Kapaza, eBay, Autoscout24, 2dehands, enz. komen veelvuldig voor. Indien je echter enkele basisregels in acht neemt en een gezonde dosis voorzichtigheid aan de dag legt, hoeft handelen via internet je niet af te schrikken.

Oplichters bespelen ook steeds vaker de gevoelige snaar in hun poging om mensen geld afhandig te maken. Hartverscheurende berichten over ***NATUURRAMPEN*** of ernstig zieke kinderen, waarbij je gevraagd wordt een gulle bijdrage te storten aan een onbekende organisatie. "Gratis" ***DIEREN*** die worden aangeboden - de eigenaar kan er niet meer voor zorgen - , en waarvoor je enkel de kosten van vervoer moet betalen.

Een nieuwe ***GELIEFDE*** of ***VRIEND*** die je via het internet hebt leren kennen, en die je vraagt om geld te sturen voor nieuwe kleren, voor de reis naar België, het paspoort, …

Of een ***BEKENDE*** (familielied, vriend, kennis,…) stuurt je een ***NOODBERICHT*** waarin hij om geld vraagt: hij zit in het buitenland en werd overvallen. Of verloor zijn portefeuille. Of raakte betrokken in een verkeersongeval… Of… Jij bent de enige die kan helpen! In werkelijkheid zit betrokkene echter gewoon thuis, en weet niets van de verstuurde noodoproep: zijn mail account werd gehackt en de oplichters hebben hetzelfde bericht naar heel zijn adresboek gestuurd.

Hou het hoofd koel, want vaak blijf jij uiteindelijk met lege handen achter!

Er zijn nog talloze andere vormen van oplichting, en soms zijn ze moeilijk te doorzien. Hieronder vind je alvast enkele tips om je beter te wapenen.

ENKELE TIPS

Algemeen

- Bescherm je computer door regelmatig updates van je besturingssysteem (vaak Windows) te installeren en steeds de laatste versie van je antivirusprogramma te gebruiken.
- Gebruik enkel originele software en werk ze geregeld bij.
- Open geen mails van mensen die je niet kent, en klik zeker niet op bijlagen in deze mails. Er kunnen alllerlei virussen in verborgen zitten die je computer ongemerkt infecteren.
- Banken of overheidsbedrijven zullen je nooit via email om je persoonlijke gegevens vragen. Wis meteen alle emails die hierom vragen. Als je echt twijfelt, neem dan contact op met de instelling in kwestie.
- Controleer namen, telefoonnummers, emailadressen van (ver)kopers of onbekende personen die je geld aanbieden via mail door ze in te geven in een zoekrobot op internet (bijvoorbeeld Google). Oplichters komen er vaak uit omdat andere slachtoffers hun verhaal doen op een of ander forum op het internet.
- Betaal NOOIT via een transfersysteem van het type Western Union of Moneygram aan een onbekende. Het zijn goede systemen om snel geld over te maken aan personen die men KENT. Maar aanvaard het niet als betalingswijze wanneer je de (ver)koper of persoon in kwestie niet kent. Deze gulden regel geldt voor alle types van oplichtingen (veilingsites, valse erfenissen, loterijen,...).

Kopen en verkopen op veilingsites/zoekertjessites

- Doe enkel aankopen wanneer je voldoende garanties krijgt dat de koper of verkoper het goed meent. Kijk bijvoorbeeld op de veilingsites naar de feedback van de (ver)koper. Het feedbacksysteem is niet waterdicht, maar geeft je toch een indicatie. Kijk ook sinds wanneer hij of zij lid is. Als hij/zij al lange tijd meegaat, is de kans groter dat het een eerlijke (ver)koper is.
- Wanneer een artikel of goed verkocht wordt aan een wel heel erg lage prijs, bijvoorbeeld een mooie ferrari aan een paar duizend euro, wees dan heel erg voorzichtig. De kans is reëel dat de (ver)koper de auto niet eens bezit en dat het om oplichting gaat.
- Geef nooit voorschotten zonder dat je het goed zelf gezien hebt. Als het zich in het buitenland bevindt, ga het dan bekijken of zoek een andere auto of artikel in eigen land.
- Als je een cheque ontvangt van een koper, doe niets tot je bank heeft bevestigd dat het een echte cheque is, die bovendien gedekt is - dit duurt enkele weken. Stort in afwachting geen geld terug aan de koper (indien hij/zij een cheque met een te hoog bedrag heeft gestuurd), en wacht met het verzenden van je koopwaar.

Valse loterijen/erfenissen

- Je kunt nooit winnen met een loterij waaraan je niet hebt deelgenomen; negeer dus alle berichten die je veel geld beloven!
- Hetzelfde geldt voor de valse erfenissen: hoe komt de zoon van wijlen de president van een Afrikaans land uitgerekend bij jou terecht? Omdat hij een spammail gestuurd heeft naar miljoenen mensen tegelijk natuurlijk. Pure oplichting!
- Maak geen afspraken met de oplichters, je riskeert niet enkel nog meer geld kwijt te raken, maar ook nog fysiek bedreigd te worden.

Emotiefraude

- Stort je bijdrage aan goede doelen die je kent. Indien je via mail wordt gecontacteerd door een gekende hulporganisatie en je wilt bijdragen, controleer dan de bankgegevens op de website van de hulporganisatie in kwestie.
- Wees alert wanneer een kandidaat-partner om geld begint te vragen.
- Werk met een erkend relatiebureau of controleer de naam van de datingsite en de gegevens van je kandidaat-partner op het internet door ze in te geven in een zoekrobot (bijvoorbeeld Google).
- Ga er niet zomaar van uit dat de afzender van een bericht via email werkelijk de persoon is die je persoonlijk kent (vriend, familie,..). Er zijn talloze manieren om zich via mail voor te doen als iemand anders.
- Wanneer je een noodbericht van een bekende ontvangt: contacteer de persoon in kwestie, zijn mail account werd vermoedelijk gehackt. Breng hem op de hoogte, zo kan hij de nodige stappen ondernemen om zijn account opnieuw over te nemen en kan hij de contacten in zijn adresboek waarschuwen voor de oplichting.

Nog meer tips vindt u onder meer op de volgende websites:
economie.fgov.be
www.eccbelgie.be
www.consumentenbedrog.be
www.web4me.be
www.saferinternet.be
www.fedpol.be (Veilig Surfen, Internetfraude)
www.westernunion.be

Misbruiken gezien? Meld ze via het meldpunt www.eCops.be

Zelf slachtoffer? Leg klacht neer bij uw plaatselijke politiedienst en neem zo veel mogelijk bewijs mee.