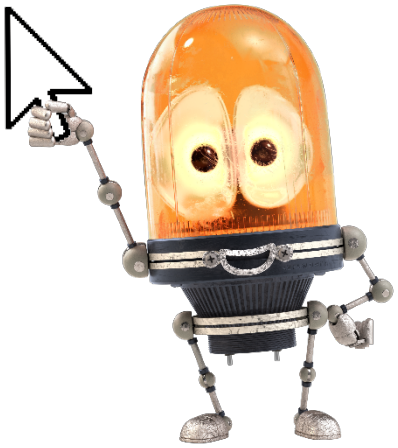
Ministerie van Justitie en Veiligheid



Communicatietoolkit
Publiekscampagne tegen internetcriminaliteit

‘Eerst checken, dan klikken’

21 mei 2019

Inleiding

Internetcriminelen worden slimmer. Daardoor is het steeds lastiger in één oogopslag te herkennen als zij je persoonlijke gegevens willen misbruiken of geld afhandig willen maken. Check daarom eerst of een link, bijlage of betaalverzoek in een e-mail, sms of appje te vertrouwen is. En klik pas als je dat zeker weet.

Om mensen te helpen zich beter tegen internetcriminaliteit te beschermen, trapt het ministerie van Justitie en Veiligheid samen met een groot aantal partners op zaterdag 25 mei 2019 een nieuwe publiekscampagne af onder het motto ‘Eerst checken, dan klikken’. Doel van de campagne is Nederlanders te bewegen basismaatregelen te nemen om zich beter tegen internetcriminelen te beschermen.

Deze toolkit helpt partners via hun eigen kanalen te communiceren over de campagne. De toolkit bestaat uit de volgende onderdelen:

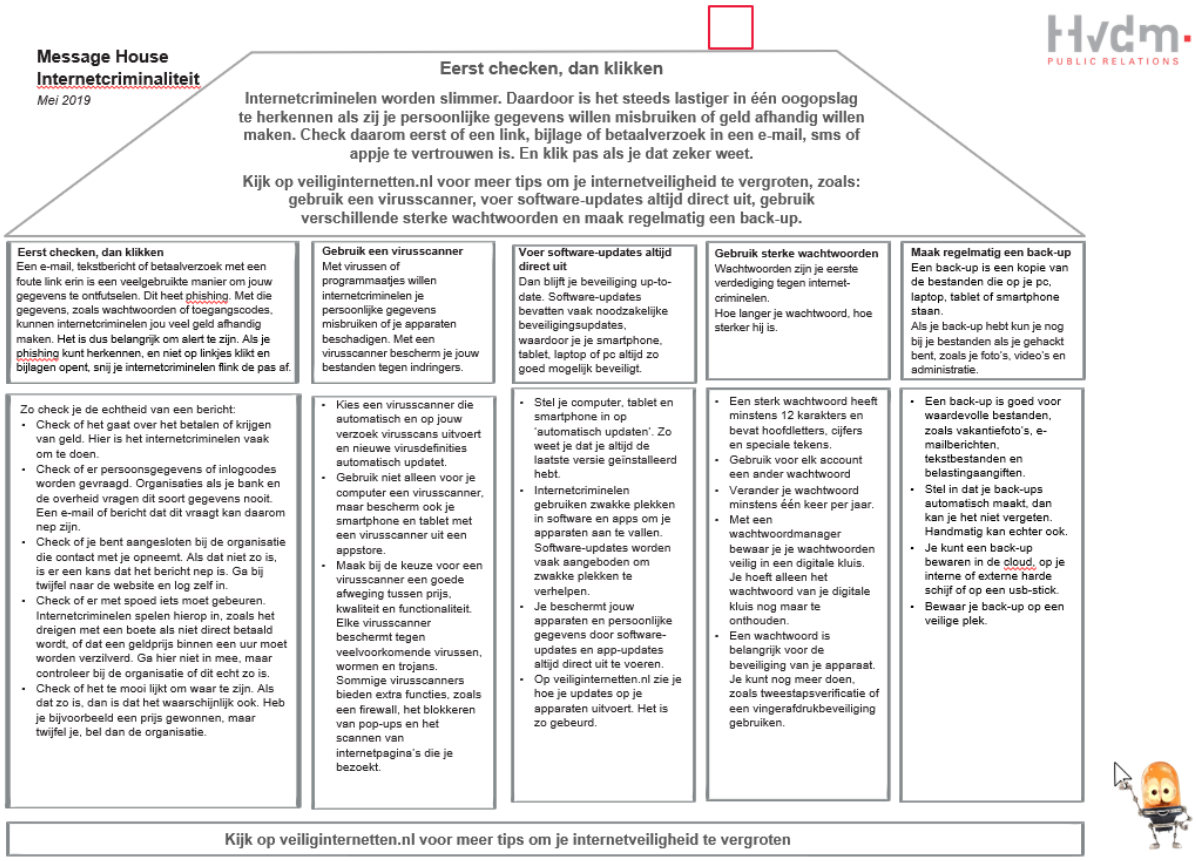
1. Message house ‘Eerst checken, dan klikken’
2. Artikel: ‘Eerst checken, dan klikken’. Wij doen mee
3. Artikel: ‘Eerst checken, dan klikken’. Zo pak je dat aan
4. Artikel: Vijf tips om jezelf te beschermen tegen internetcriminelen
5. Artikel: Wat moet je doen als het toch misgaat?
6. Artikel: Slimme links
7. Artikel: Valse sms’jes populair onder internetcriminelen
8. Ervaringsverhaal: Irene van den Berg, slachtoffer van ransomware
9. Feiten & cijfers
10. Voorbeelden social posts
11. Beeldmateriaal

Bij vragen over deze toolkit of de campagne kun je contact opnemen met onderstaand contactpersoon.

Contactpersoon
Dennis Cohen
Communicatieadviseur
Ministerie van Justitie en Veiligheid
d.cohen@minjenv.nl

1. Message house

Dit message house bevat de kerninformatie om mensen te informeren hoe zij zich beter tegen internetcriminaliteit kunnen beschermen.



Message House
Internetcriminaliteit
Mei 2019

Eerst checken, dan klikken

Internetcriminelen worden slimmer. Daardoor is het steeds lastiger in één oogopslag te herkennen als zij je persoonlijke gegevens willen misbruiken of geld afhandig willen maken. Check daarom eerst of een link, bijlage of betaalverzoek in een e-mail, sms of appje te vertrouwen is. En klik pas als je dat zeker weet.

Kijk op veiliginternetten.nl voor meer tips om je internetveiligheid te vergroten, zoals: gebruik een virusscanner, voer software-updates altijd direct uit, gebruik verschillende sterke wachtwoorden en maak regelmatig een back-up.

Eerst checken, dan klikken
Een e-mail, tekstbericht of betaalverzoek met een foute link erin is een veelgebruikte manier om jouw gegevens te ontfutselen. Dit heet phishing. Met die gegevens, zoals wachtwoorden of toegangscodes, kunnen internetcriminelen jou veel geld afhandig maken. Het is dus belangrijk om alert te zijn. Als je phishing kunt herkennen, en niet op linkjes klikt en bijlagen opent, snij je internetcriminelen flink de pas af.

Zo check je de echtheid van een bericht:
- Check of het gaat over het betalen of krijgen van geld. Hier is het internetcriminelen vaak om te doen.
- Check of er persoonsgegevens of inlogcodes worden gevraagd. Organisaties als je bank en de overheid vragen dit soort gegevens nooit. Een e-mail of bericht dat dit vraagt kan daarom nep zijn.
- Check of je bent aangesloten bij de organisatie die contact met je opneemt. Als dat niet zo is, is er een kans dat het bericht nep is. Ga bij twijfel naar de website en log zelf in.
- Check of er met spoed iets moet gebeuren. Internetcriminelen spelen hierop in, zoals het dreigen met een boete als niet direct betaald wordt, of dat een geldprijs binnen een uur moet worden verzilverd. Ga hier niet in mee, maar controleer bij de organisatie of dit echt zo is.
- Check of het te mooi lijkt om waar te zijn. Als dat zo is, dan is dat het waarschijnlijk ook. Heb je bijvoorbeeld een prijs gewonnen, maar twijfel je, bel dan de organisatie.

Gebruik een virusscanner
Met virussen of programmaatjes willen internetcriminelen je persoonlijke gegevens misbruiken of je apparaten beschadigen. Met een virusscanner bescherm je jouw bestanden tegen indringers.

- Kies een virusscanner die automatisch en op jouw verzoek virusscans uitvoert en nieuwe virusdefinities automatisch updatet.
- Gebruik niet alleen voor je computer een virusscanner, maar bescherm ook je smartphone en tablet met een virusscanner uit een appstore.
- Maak bij de keuze voor een virusscanner een goede afweging tussen prijs, kwaliteit en functionaliteit. Elke virusscanner beschermt tegen veelvoorkomende virussen, wormen en trojans. Sommige virusscanners bieden extra functies, zoals een firewall, het blokkeren van pop-ups en het scannen van internetpagina's die je bezoekt.

Voer software-updates altijd direct uit
Dan blijft je beveiliging up-to-date. Software-updates bevatten vaak noodzakelijke beveiligingsupdates, waardoor je je smartphone, tablet, laptop of pc altijd zo goed mogelijk beveiligt.

- Stel je computer, tablet en smartphone in op 'automatisch updaten'. Zo weet je dat je altijd de laatste versie geïnstalleerd hebt.
- Internetcriminelen gebruiken zwakke plekken in software en apps om je apparaten aan te vallen. Software-updates worden vaak aangeboden om zwakke plekken te verhelpen.
- Je beschermt jouw apparaten en persoonlijke gegevens door software-updates en app-updates altijd direct uit te voeren.
- Op veiliginternetten.nl zie je hoe je updates op je apparaten uitvoert. Het is zo gebeurd.

Gebruik sterke wachtwoorden
Wachtwoorden zijn je eerste verdediging tegen internet-criminelen.
Hoe langer je wachtwoord, hoe sterker hij is.

- Een sterk wachtwoord heeft minstens 12 karakters en bevat hoofdletters, cijfers en speciale tekens.
- Gebruik voor elk account een ander wachtwoord
- Verander je wachtwoord minstens één keer per jaar.
- Met een wachtwoordmanager bewaar je je wachtwoorden veilig in een digitale kluis. Je hoeft alleen het wachtwoord van je digitale kluis nog maar te onthouden.
- Een wachtwoord is belangrijk voor de beveiliging van je apparaat. Je kunt nog meer doen, zoals tweestapsverificatie of een vingerafdrukbeveiliging gebruiken.

Maak regelmatig een back-up
Een back-up is een kopie van de bestanden die op je pc, laptop, tablet of smartphone staan.
Als je back-up hebt kun je nog bij je bestanden als je gehackt bent, zoals je foto's, video's en administratie.

- Een back-up is goed voor waardevolle bestanden, zoals vakantiefoto's, e-mailberichten, tekstbestanden en belastingaangiften.
- Stel in dat je back-ups automatisch maakt, dan kan je het niet vergeten. Handmatig kan echter ook.
- Je kunt een back-up bewaren in de cloud, op je interne of externe harde schijf of op een usb-stick.
- Bewaar je back-up op een veilige plek.

Kijk op veiliginternetten.nl voor meer tips om je internetveiligheid te vergroten

Het message house is hier als PDF te downloaden.

2. Artikel: ‘Eerst checken, dan klikken’. Wij doen mee

Dit artikel kun je gebruiken om aan te kondigen dat jouw organisatie meedoet aan de campagne ‘Eerst checken, dan klikken’, bijvoorbeeld via een nieuwsbrief.

‘Eerst checken, dan klikken’. Wij doen mee
Internetcriminelen worden slimmer. Daardoor is het steeds lastiger in één oogopslag te herkennen als zij je persoonlijke gegevens willen misbruiken of geld afhandig willen maken. Check daarom eerst of een link, bijlage of betaalverzoek in een e-mail, sms of appje te vertrouwen is. En klik pas als je dat zeker weet.

Om mensen te helpen zich beter tegen internetcriminaliteit te beschermen, trapt het ministerie van Justitie en Veiligheid samen met een groot aantal partners op zaterdag 25 mei 2019 een nieuwe publiekscampagne af onder het motto ‘Eerst checken, dan klikken’. Ook wij doen mee.

Hier kun je de activiteiten van jouw organisatie invoegen.

Op veiliginternetten.nl vind je tips om je internetveiligheid verder te vergroten. Ook kun je een quiz spelen om jouw kennis te testen.

Over de campagne
Met de publiekscampagne tegen internetcriminaliteit wil het ministerie van Justitie en Veiligheid Nederlanders helpen zich beter tegen internetcriminaliteit te beschermen. De campagne is zichtbaar op TV en sociale media. Daar worden mensen opgeroepen maatregelen te treffen tegen internetcriminaliteit. Verder ondersteunen diverse bedrijven en organisaties uit onder meer de ICT- en telecomsector de publiekscampagne. Zij vragen via hun eigen kanalen aandacht voor het onderwerp.

3. Artikel: ‘Eerst checken, dan klikken’. Zo pak je dat aan

Dit artikel vertelt lezers hoe zij alerter kunnen handelen op internet. Je kunt dit artikel plaatsen op je website, meenemen op sociale kanalen of toevoegen aan een nieuwsbrief.

‘Eerst checken, dan klikken’. Zo pak je dat aan
We horen het regelmatig in het nieuws: er worden heel wat nepmails verstuurd. Internetcriminelen proberen op die manier persoonlijke gegevens van je te krijgen en te misbruiken. Door eerst een link, bijlage of betaalverzoek in een e-mail, sms of appje te checken op betrouwbaarheid, voorkom je dat jij slachtoffer wordt. En weet je zeker dat een link veilig is.

Maar hoe pak je dat aan? En wat moet je checken?

- Check of het gaat over geld. Hier is het internetcriminelen vaak om te doen.
- Check of er persoonsgegevens of inlogcodes worden gevraagd. De bank of de overheid vraagt hier nooit om. Een e-mail of bericht waarin dit wordt gevraagd, kan daarom nep zijn.
- Check of je bent aangesloten bij de organisatie die contact met je opneemt. Als dat niet zo is, is er een kans dat het bericht nep is. Ga bij twijfel naar de website en log zelf in.
- Check of er spoed is. Internetcriminelen spelen hierop in. Ga hier niet in mee, maar controleer bij de organisatie of dit echt zo is.
- Check of het te mooi lijkt om waar te zijn. Lijkt iets te mooi, dan is dat het waarschijnlijk ook zo. Heb je bijvoorbeeld een prijs gewonnen, maar twijfel je, bel dan de organisatie.

Bij een e-mail geldt ook:
- Check de aanhef. Hoe algemener en onpersoonlijker, hoe groter de kans dat het niet echt is.

- Check de afzender. Internetcriminelen maken vaak een e-mailadres of website na die héél erg lijkt op het origineel, maar dat niet is.
- Check de bijlage(n). Ontvang je een mail met bijlagen, open deze dan niet, zeker geen bijlagen met de extensie '.exe'.

Bij WhatsApp en sms-berichten geldt ook:
- Check of je de persoon kent. Vertrouw je het niet? Neem dan contact op met de afzender.
- Check of het écht klopt. Als een vriend of familielid opeens om (veel) geld vraagt, bel degene even. Een crimineel die het nummer misbruikt, valt bij bellen door de mand.
- Check of je de organisatie kent. Kijk voor de zekerheid op de website van de organisatie.
- Check of je persoonlijke gegevens deelt via sociale media. Internetcriminelen kunnen bijvoorbeeld je telefoonnummer vinden en misbruiken.

Bij een betaalverzoek geldt:
- Check of je wel echt geld verschuldigd bent aan degene die jou een appje stuurt.
- Check of je degene kunt bellen die je een appje of betaalverzoek stuurt. Maak nooit direct geld over.

Mocht je een e-mail, bericht of betaalverzoek ontvangen waarover je twijfelt, houd dan altijd de volgende regels aan.
- Klik niet op linkjes.
- Klik niet op bijlagen.
- Maak het gevraagde bedrag niet over.
- Neem contact op met de organisatie die volgens de e-mail iets van je wil. Zoek de contactgegevens zelf op, gebruik niet die van de e-mail waaraan je twijfelt. De organisatie zal je kunnen vertellen of bijvoorbeeld het openstaande bedrag nog betaald moet worden, of dat het een nepbericht is.
- Log niet in via de link in de e-mail. Ga zelf naar de vertrouwde app of typ zelf het adres van de organisatie in. Als het bericht echt is, zal je het hoogstwaarschijnlijk in je inbox op die website zien staan.
- Check de link op checkjelinkje.nl. Doe dit door de link te kopiëren, niet door erop te klikken!

Door eerst te checken en dan pas te klikken, voorkom je dat jij slachtoffer wordt van internetcriminaliteit. Maar wat moet je doen als het toch misgaat? Daarover lees je hier meer.

Kijk op veiliginternetten.nl voor meer tips om je internetveiligheid te vergroten.

4. Artikel: Vijf tips om jezelf te beschermen tegen internetcriminelen

Dit artikel gaat dieper in op vijf tips om de lezer te beschermen tegen internetcriminelen. De tips kun je ook afzonderlijk gebruiken als posts voor op sociale media.

Vijf tips om jezelf te beschermen tegen internetcriminelen
E-mails, tekstberichten en betaalverzoeken, ze kunnen zomaar foute links bevatten. We noemen deze vorm van internetcriminaliteit phishing. Het zijn veelgebruikte manieren om jouw gegevens te ontfutselen. Met die gegevens kunnen internetcriminelen jou geld afhandig maken, of ervandoor gaan met je identiteit. Als je phishing kunt herkennen, en niet op linkjes en bijlagen klikt, snij je internetcriminelen flink de pas af. In dit artikel leggen wij je uit hoe jij je beschermt tegen phishing en andere vormen van internetcriminaliteit.

Eerst checken, dan klikken
Klik niet zomaar op iedere link of bijlage, maar controleer de echtheid van een e-mail, appje of betaalverzoek om phishing te voorkomen. In artikel 3 leggen we je uit hoe je dat doet.

Gebruik verschillende sterke wachtwoorden
Wachtwoorden zijn je eerste verdediging tegen internetcriminelen. Gebruik daarom sterke en unieke wachtwoorden per dienst. Deze zijn moeilijker te kraken en mocht er ooit iemand achter je wachtwoord van een bepaalde dienst komen, dan hoef je alleen dat wachtwoord te veranderen. Om jezelf nog beter te beschermen, kun je soms ook kiezen voor tweestapsverificatie of vingerafdrukbeveiliging. Bij tweestapsverificatie voeg je naast een wachtwoord een extra check toe, bijvoorbeeld doordat je ook een code moet invoeren die je ontvangt in een sms.

Hoe maak ik een sterk wachtwoord?
- Hoe langer je wachtwoord, hoe sterker het is. Het liefst langer dan acht tekens.
- Gebruik ook cijfers en speciale tekens (zoals ! $ ^ & #)
- Zorg dat je kleine letters én hoofdletters gebruikt.
- Gebruik een wachtzin, zoals: MijnHondHeeft4PotenEn1Staart! Die zijn makkelijker te onthouden en ook nog lang.
- Gebruik een wachtwoordmanager om je wachtwoorden te kunnen onthouden, of schrijf deze op in een boekje.

Wat is <u>geen</u> sterk wachtwoord?
- 123456
- !@#$%^
- Johan1994
- Iloveyou
- qwerty
- admin
- wachtwoord123

Om te checken hoe sterk jouw wachtwoord is, surf je naar
https://veiliginternetten.nl/wachtwoordkraak-test/

Voer software-updates altijd direct uit
Een software-update installeert een nieuwe versie van het besturingssysteem van je apparaat. Software-updates bevatten vaak beveiligingsupdates waardoor je gegevens beter beschermd blijven. Installeer daarom altijd direct alle software- en app-updates op je computer, tablet en mobiele telefoon.

Tips voor software-updates:
- Controleer of je de laatste update geïnstalleerd hebt

- Stel je computer, telefoon en tablet in op ‘automatisch updaten’. Zo weet je dat je altijd de laatste versie geïnstalleerd hebt.

Gebruik altijd een virusscanner
Met virussen of programma’s willen internetcriminelen je persoonlijke gegevens misbruiken of je apparaten beschadigen. Een virusscanner beschermt je daartegen en scant je computer op virussen en andere schadelijke bestanden. Daarmee is het een belangrijk onderdeel van de bescherming van je computer. Je kunt betaalde of onbetaalde virusscanners installeren. Een betaalde virusscanner heeft vaak meer functies dan een gratis versie. Toch is het beter om een gratis virusscanner te hebben dan helemáál geen virusscanner.

Virusscanners voor tablets en smartphones zijn bij appstores verkrijgbaar. Een virusscanner checkt elke app die je installeert en geeft je een waarschuwing als de app kwaadaardig is. Wel geldt bij het gebruik van een virusscanner nog steeds dat je zelf moet blijven opletten bij het downloaden van apps.

Tips over virusscanners:
- Installeer sowieso een gratis virusscanner, dan kan je later altijd nog beslissen een betaalde versie te gebruiken.
- Kijk hieronder hoe je een goede virusscanner uit kunt kiezen.

Maak regelmatig een back-up
Een back-up is een kopie van je gegevens op een veilige plek. Zo voorkom je dat je foto's, werkstukken en alle andere bestanden op je computer kwijt bent als je computer bijvoorbeeld besmet raakt met een virus. En vergeet ook de bestanden op je mobiele telefoon en tablet niet.

Zorg er tot slot voor dat je een back-up op een veilige plek bewaart.

Kijk op veiliginternetten.nl voor meer tips om je internetveiligheid te vergroten.

5. Artikel: Wat moet je doen als het toch misgaat?
Dit artikel geeft tips aan mensen die per ongeluk tóch op een verkeerde link of bijlage hebben geklikt. Je kunt dit artikel gebruiken op de website of als nieuwsbriefitem.

Wat moet je doen als het toch misgaat?
Het zal je maar gebeuren. In een onoplettend moment klik je per ongeluk een verkeerde link of open je een bijlage. Direct verschijnt een pop-up met de boodschap dat je geld moet betalen. Wat doe je dan?

- Raak om te beginnen niet in paniek. Door rustig te blijven, kun je helder nadenken.
- Neem direct contact op met de organisatie waarvan de gegevens misbruikt worden. Ga naar de website van de organisatie om een telefoonnummer of e-mailadres te vinden, gebruik niet de contactgegevens uit de e-mail waar je in bent getrapt. Maak melding van wat er is en vraag hoe je dit het beste kunt herstellen.
- Doe aangifte bij de politie.
- Als het om een wachtwoord gaat, verander dit dan direct.
- Meld phishing e-mails, appjes en betaalverzoeken bij de Fraude Helpdesk. Zo kun je voorkomen dat anderen ook slachtoffer worden.
- Voer een virusscan uit.

Kijk op veiliginternetten.nl voor meer tips om je internetveiligheid te vergroten.

6. Artikel: Slimme links voor meer online veiligheid

Dit artikel geeft lezers die meer willen weten óf zich beter willen wapenen tegen internetcriminelen een aantal slimme links waarvan zij kunnen leren. Die slimme links kun je ook gebruiken voor je sociale posts.

Slimme links voor meer online veiligheid
Internetcriminelen worden slimmer. Daardoor is het steeds lastiger in één oogopslag te herkennen als zij je persoonlijke gegevens willen misbruiken of geld afhandig willen maken. Check daarom eerst of een link, bijlage of betaalverzoek in een e-mail, sms of appje te vertrouwen is. En klik pas als je dat zeker weet.

Je kunt hier voldoende informatie over vinden. In de onderstaande links vind je bijvoorbeeld een quiz die je helpt phishing te herkennen, hoe je een wachtwoordmanager instelt en een handige tool die je helpt links te checken die je niet helemaal vertrouwt. Ze zijn allemaal veilig.

Checkjelinkje.nl: controleer links op echtheid (ook beschikbaar op iPhone en iPad)
Google Phishing Quiz: herken jij de phishingpoging?
Veiliginternetten.nl: geeft je advies over veilig internetgebruik
Laatjeniethackmaken.nl: handleiding die op een begrijpelijke manier uitlegt hoe je jezelf beschermt tegen hackers.
veiliginternetten.nl/wachtwoordkraak-test/: check hoe makkelijk jouw wachtwoord te kraken is.

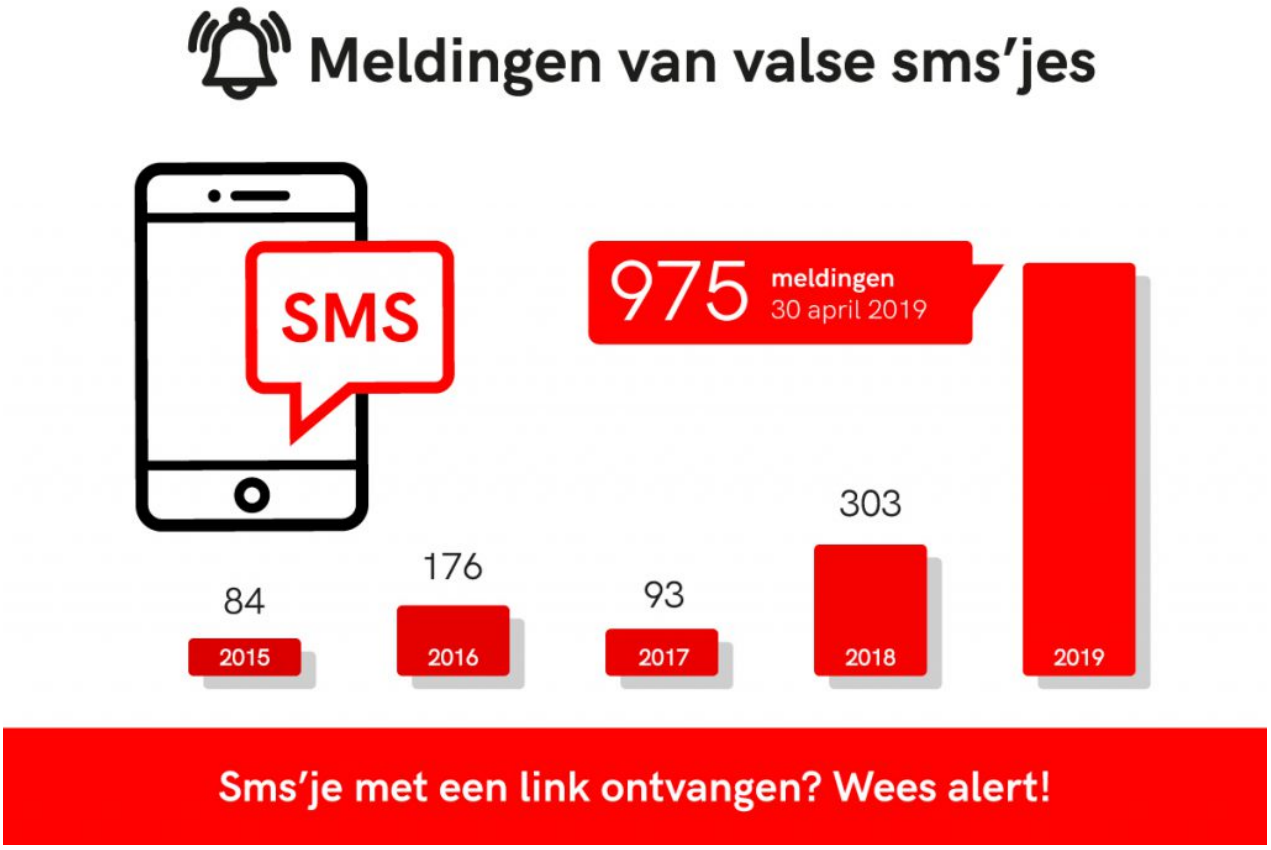
Kijk op veiliginternetten.nl voor meer tips om je internetveiligheid te vergroten.

7. Artikel: Valse sms'jes populair onder internetcriminelen

Dit artikel gaat in op valse sms'jes. Internetcriminelen gebruiken dit middel steeds vaker om toegang te krijgen tot persoonlijke gegevens of bankinformatie.

Valse sms'jes populair onder internetcriminelen
Internetcriminelen versturen steeds meer sms-berichten om mensen op te lichten. In 2017 ontving de Fraudehelpdesk 93 meldingen, in de eerste vier maanden van dit jaar zijn dat er al 975! Ontvang jij een sms van een onbekende en bevat dit bericht een link? Check dan eerst de afzender en klik pas als je zeker weet dat de link betrouwbaar is.

Regelmatig gaat het om nep-boetes, bijvoorbeeld uit naam van het CJIB. Ontvangers krijgen een sms over een openstaande boete met daarin een echte betaallink. Via de link ga je echt naar de bank en betaal je de zogenaamde boete. Alleen betaal je niet aan het CJIB, maar aan de oplichter.



Bron: Fraudehelpdesk.nl

Ook phishing-berichten zijn populair, bijvoorbeeld namens de bank. Fraudeurs proberen achter je inloggegevens te komen door bijvoorbeeld te dreigen met het blokkeren van je rekening of met het afschrijven van een groot bedrag.

Klik je op de link, dan kom je terecht op een nepwebsite die nauwelijks van echt te onderscheiden is. Als je inlogt, worden de gegevens direct doorgestuurd aan de internetcrimineel. Met deze gegevens probeert de oplichter vervolgens je bankrekening te plunderen.

Eerst checken, dan klikken
Ontvang je een boete, rekening of ander betaalverzoek per sms, WhatsApp of e-mail? Bel dan altijd ter controle! Betaal nooit een rekening op basis van alleen een tekstbericht. En moet je écht iets overmaken? Tik de link dan zelf in en klik hem niet aan.

Wil je zeker weten dat het webadres klopt? Ga naar checkjelinkje.nl en kopieer de link hierin. En kijk op veiliginternetten.nl voor meer tips om je internetveiligheid te vergroten.

8. Ervaringsverhaal: Irene van den Berg, slachtoffer van ransomware

“Ik was alles kwijt”
Freelance journaliste Irene van den Berg kende de trucs van internetcriminelen en toch ging het mis. Terwijl ze druk aan het werk was, klikte ze op een valse link en raakte al haar bestanden kwijt.

“Ik werkte aan een column en kreeg een mail binnen van mijn telecomprovider. Daarin stond dat er een factuur voor mij klaarstond. Het bedrag was veel hoger dan normaal. Ik was net op vakantie geweest dus ik was bang dat ik daar per ongeluk veel verbruikt had. Ik klikte op de link om de specificatie te bekijken en kwam niet op de site van de provider. Mijn eerste gedachte: Shit, dit had ik niet moeten doen.”

Irene klikte de website weg, maar het was al te laat. Na een half uur verscheen er een pop-up met een dreigende tekst. “Ik zit met meerdere ZZP’ers in een ruimte, dus toen ik uitleg gaf bij mijn boze uitroep, riep een IT-er meteen: ‘Zet je computer uit!’ Ik schrok en deed wat hij zei.”

Alles kwijt
Met de klik op de valse link, haalde Irene onbedoeld ransomware binnen. Dat is kwaadaardige software die de bestanden op de computer gijzelt. “Het bericht op mijn computer meldde dat ik een Bitcoin (die was toen ongeveer 600 euro waard) moest betalen om weer toegang te krijgen tot al mijn bestanden. Eigenlijk had ik drie opties. Ik kon de criminelen betalen, een bureau inschakelen om de code te kraken of ik was alles kwijt. Optie 1 viel meteen af vanwege morele overwegingen. Optie 2 is ook onzeker; je weet nooit of het lukt en je bent geld kwijt aan het bureau. Bleef over: optie 3, alles kwijt.”

Niet alleen was al het werk van Irene weg, ook haar mails, vakantiefoto’s en contacten waren kwijt. “Dat was privé, maar ook als ZZP’er een nogal vervelende situatie. Ik heb daarna meteen maatregelen getroffen. Mijn nieuwe harde schijf heeft nu goede antivirussoftware. Ik maak vaker een back-up van mijn bestanden en ben echt heel voorzichtig met klikken op links. Ik check eerst of een link wel te vertrouwen is.”

Irene heeft zeker haar lesje geleerd, maar durft niet te zeggen dat het haar nooit meer overkomt. “Hoewel ik wist hoe internetcriminelen werken en er zelfs over heb geschreven, wisten ze me toch te verrassen op een onbewaakt moment. Mijn eerste reactie was: ‘hoe stom kun je zijn?!’ Maar ja, het blijkt maar weer: internetcriminaliteit kan echt iedereen overkomen.”

Kijk op veiliginternetten.nl voor meer tips om je internetveiligheid te vergroten.

9. Feiten & cijfers

Deze feiten en cijfers kun je benutten in artikelen of posts die je zelf maakt.

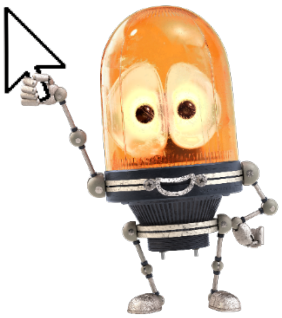
- In 2017 was een op de negen Nederlanders slachtoffer van een vorm van internetcriminaliteit. Het gaat hierbij om identiteitsfraude, koop- en verkoopfraude, hacken of cyberpesten (CBS, 2018).
- Bijna de helft van de Nederlanders (44%) maakt zich weleens zorgen dat hij of zij zelf te maken krijgt met een cyberaanval. Jongeren (19 t/m 34 jaar) en hoogopgeleiden zijn hier vaker onbezorgd over (AlertOnline, 2018).
- Vier op de tien werkende Nederlanders hebben behoefte aan verbetering van hun persoonlijke online veiligheid (AlertOnline, 2018).
- Het grootste risico om slachtoffer te worden van internetcriminaliteit loop je volgens Nederlanders als je een link in een e-mail aanklikt, een bijlage van een e-mail opent, als je bestanden downloadt van internet of als je op een openbare computer zit (AlertOnline, 2018).
- Circa zes op de tien Nederlanders (57%) denken dat als er een groen slotje en/of https voor het adres van de website staat, de website veilig te bezoeken is. Terwijl het slotje staat voor een beveiligde verbinding. De websites kunnen nog steeds malafide websites zijn (AlertOnline, 2018).

10. Social posts

- Internetcriminelen worden slimmer. Om mensen te beschermen tegen valse links, bijlages en betaalverzoeken, organiseren wij samen met het ministerie van Justitie en Veiligheid de campagne ‘Eerst checken, dan klikken’. Meer weten? Ga naar www.veiliginternetten.nl. #eerstcheckendanklikken
- Internetcriminelen worden steeds slimmer. Ben jij ze te slim af? Doe de Phishing Quiz, Check je linkje en Laat je niet hack maken! Meer informatie op www.veiliginternetten.nl. #eerstcheckendanklikken
- Internetcriminelen worden steeds slimmer. Weet jij wat je moet doen om ze buiten de deur te houden? Doe de quiz! [link naar quiz veiliginternetten.nl] #eerstcheckendanklikken
- Wachtwoorden zijn je eerste verdediging tegen internetcriminelen. Check hier hoe makkelijk jouw wachtwoord te kraken is: https://veiliginternetten.nl/wachtwoordkraak-test/ #eerstcheckendanklikken

Campagnehashtag: #eerstcheckendanklikken

11. Beeldmateriaal

Aanvullend beeldmateriaal is hier te downloaden.