Preventie cybercriminaliteit

Veilig op w.w.w.

10 TIPS

Stijn van Bouwel

Politie

Gouverneur
Provincie Antwerpen
Cathy Berx

provincie gouverneur
Vlaams-Brabant
Jan Spooren

KORTRIJK

KALMTHOUT
als je van natuur houdt

KMO-zone
Bosduin vzw

Kapellen

BIN
Kenniscentrum
Buurt.Informatie.Netwerk

PREVENTIETIPS

Ongetwijfeld gebruik je preventieve maatregelen om je computer, smartphone, tablet e.a. te beveiligen tegen cybercriminaliteit en denk je dat het goed is, maar het kan nog beter, zeker weten...

10 TIPS

1. Gebruik complexe wachtwoorden en/of lange wachtwoordzinnen.
2. Kies indien mogelijk voor tweestapsverificatie.
3. Installeer altijd de officiële software-updates. Maak regelmatig back-ups van je bestanden.
4. Installeer een antivirusprogramma.
5. Open geen berichten en onbekende bestanden die je niet verwacht of vertrouwt.
6. Installeer alleen apps via de officiële applicatiewinkels
7. Controleer het adres van websites op onregelmatigheden.
8. Verbreek het contact met ongevraagde helpdeskmedewerkers.
9. Stel je privacyinstelling zo hoog mogelijk in op sociale media.
10. Maak alleen verbinding met vertrouwde wifinetwerken, liefst geen publieke wifinetwerken.

TIP
1

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

Wachtwoorden

- Gebruik complexe wachtwoorden en/of lange wachtwoordzinnen.
- Gebruik nooit hetzelfde wachtwoord voor verschillende toepassingen.
- Verander regelmatig je wachtwoord.
- Gebruik een wachtwoordkluis *of wachtwoordenboekje als geheugensteun.*
- *Bewaar het boekje op een veilige plaats en niet naast je computer.*

TIP
1

WACHTWOORDTIPS

Een wachtwoord moet lang en uniek zijn om geautomatiseerde aanvallen van criminelen af te weren. Met moderne technieken kunnen ze soms miljarden wachtwoorden per seconde proberen. De volgende tips maken je wachtwoorden moeilijker te kraken:

- ✓ **Hoe meer tekens, des te veiliger**. Acht tekens is aan de korte kant. Het is verstandiger een lengte van minimaal 12 tekens aan te houden. Dat maakt het wachtwoord tot 80 miljoen keer zo sterk. Maar meer tekens is nog beter.
- ✓ **Cijfers, hoofdletters en speciale tekens** (&, ?, #, !, %, enz.) versterken het wachtwoord.
- ✓ Of gebruik **een wachtzin**, die onthoud je makkelijker. Voorbeeld: IkHeb100Fietspompen.
- ✓ Gebruik wachtzinnen van **minimaal 4 woorden**. Gebruik geen spreekwoord of bekende zin. Voorbeeld: 131KilometerIsTeSnel. Het wachtwoord mag geen makkelijk te raden **persoonlijke informatie** bevatten, zoals een naam, geboortedatum of adres.
- ✓ Gebruik **verschillende wachtwoorden** voor elke website en dienst.
- ✓ Pas wachtwoorden minimaal **1 keer per jaar** aan. Niet te vaak, want je moet het wel kunnen onthouden.
- ✓ Controleer eens in de zoveel tijd of je inloggegevens niet in verkeerde handen gevallen zijn, bijvoorbeeld op haveibeenpwned.com. Steeds meer wachtwoordkluizen kunnen ook zo'n check uitvoeren.

Bron: Consumentenbond

BIN Kenniscentrum Buurt.Informatie.Netwerk
Politie
Gouverneur Provincie Antwerpen Cathy Berx
provincie gouverneur Vlaams-Brabant
KORTRIJK

TIP

1

Tekens	Mogelijke combinaties	Tijd nodig
1	62	<1 seconde
2	3.844	<1 seconde
3	238.328	<1 seconde
4	14.776.336	< 1 seconde
5	916.132.832	42 seconden
6	56.800.235.584	43 minuten
7	3.521.614.606.208	44 uur
8	218.340.105.584.896	115 dagen
9	13.537.086.546.263.600	20 jaren
10	839.299.365.868.340.000	12 eeuwen
11	52.036.560.683.837.100.000	750 eeuwen
12	3.226.266.762.397.900.000.000	46500 eeuwen
Aantal mogelijke karakters: 62 (A-Z, a-z, 0-9) Aantal passwords per minuut +/- 22.000.000		

Meest gebruikte wachtwoorden

123456	azertyuiop	voetbal
azerty	loulou	azerty123
7153	charlotte	caroline
123456789	123123	qwerty
1234	standard	isabelle
12345	wachtwoord	computer
abc123	thomas	sloeber
password	nathalie	azerty1
anderlecht	111111	bolleke
12345678	telenet1	paswoord

TIP
2

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

Kies indien mogelijk voor tweestapverificatie.

Al heel wat bedrijven en instellingen bieden deze mogelijkheid aan.

TIP
2

WACHTWOORDTIPS

Welke wachtwoordmethode je ook hanteert, wachtwoorden kunnen door een datalek of hack soms toch in verkeerde handen vallen. Gebruik daarom ook Two Factor Authentication (2FA) of tweestapverificatie – Wat is het ?

Om toegang te krijgen tot je account moet je bewijzen dat je bent wie je beweert te zijn. Dat kan op 3 manieren of met 3 factoren:

- ✓ met iets dat jij alleen weet (jouw wachtwoord of pincode),
- ✓ met iets dat jij alleen hebt (jouw telefoon of token),
- ✓ met iets dat jij bent (jouw vingerafdruk, gezicht, iris…).

Je gebruikt best twee- of meerstapverificatie (2FA of MFA). Je hebt dan bvb een wachtwoord en je laat daar bovenop ook **een code naar je GSM** sturen, of je gebruikt je **vingerafdruk** en een app om toegang te krijgen.

De meest gebruikte diensten bieden een vorm van tweestapverificatie aan en hebben een korte instructiepagina.

Bron: SafeonWeb

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

TIP **3**

- Installeer altijd de officiële software-updates. Zo verklein je de kans dat je gehackt wordt.
- Maak (voor je update bv) regelmatig back-ups van je bestanden.

TIP **4**

- Installeer een antivirusprogramma op al je toestellen en niet alleen op je computer/laptop.
- Schakel automatische updates in voor je antivirusprogramma en je software.
- Maak ook gebruik van een firewall.

BIN Kenniscentrum Buurt.Informatie.Netwerk
Politie
Gouverneur Provincie Antwerpen Cathy Berx
provincie gouverneur Vlaams-Brabant
KORTRIJK

TIP
5

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

Open geen berichten en onbekende bestanden die je niet verwacht of vertrouwt.

TIP
5

10 TIPS

Een bericht dat je niet verwacht met een bestand in de bijlage ?

Dit lijkt zeer sterk op
PHISHING !

Phishing is een **vorm van online fraude** waarbij slachtoffers criminelen toegang geven tot hun persoonlijke informatie of bankrekening. Vaak gebeurt dit in de vorm van een e-mail die afkomstig lijkt te zijn van een officiële instantie, organisatie of bedrijf. Door middel van een techniek genaamd social engineering *(het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid.)* proberen criminelen vertrouwelijke informatie van iemand los te krijgen en **doen deze oplichters zich voor als een betrouwbare bron**, maar het doel is om je geld of persoonsgegevens buit te maken.

Bron: safeonweb

TIP
5

10 TIPS


Phishing checklist
Hoe een valse mail herkennen?
Let op voor deze 9 signalen. Hoe meer je er herkent, hoe groter de kans dat het bericht vals is.
Is het onverwacht?
Is het dringend?
Ken je de afzender?
Vind je de vraag vreemd?
Naar waar leidt de link?
Bevat het bericht veel taalfouten?
Word je persoonlijk aangesproken?
Zit het bericht in je Spam/Junk folder?
Wordt er gevraagd om een betaling uit te voeren?

TIP
6

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

Installeer alleen apps via de officiële applicatiewinkels.

Playstore voor Android
Applestore voor IoS
Windows Store voor Microsoft

TIP
7

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

Controleer het adres (URL) van websites

Een internetadres is iets uniek. Kijk deze goed na.
En “https” wilt niet per definitie zeggen dat je website veilig is.
De verbinding is “beveiligd”, zo ook kunnen cybercriminelen een valse website aanmaken en zo hun website “beveiligen”

Een andere tactiek van oplichters zijn spelfouten (homogliefen).
www.micosoft.com
www.microsoft.com
www.mircosoft.com

Of de letter o vervangen door het nummer 0
www.yah00.com

Of de letter l vervangen door de letter i:
http://vlaanderen.beiasting.info/

TIP 7

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

Hoe voorkomen?

- Niet klikken, maar typen (m.b.t. bekende webadressen).
- Indien je moet betalen, ga zelf naar de algemene website van je internetbank via bv. Google.

- Je kan de legitimiteit van een link verifiëren in een tool: https://www.scamadviser.com/nl/home

Webshops zijn niet altijd betrouwbaar. Controle van de site in kwestie kost wat moeite maar kan je het verlies van veel geld besparen.
Twijfel je ? Aarzel niet en doe de WebshopCheck thuis

Hulp en advies aan consumenten in Europa
ECC-Net
Europees Centrum voor de Consument België

BIN Kenniscentrum Buurt.Informatie.Netwerk

Politie

Gouverneur Provincie Antwerpen Cathy Berx

provincie gouverneur Vlaams-Brabant

KORTRIJK

TIP
8

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

HELPDESKFraude - Oplichters doen zich voor als helpdeskmedewerkers van MS, Apple of andere computerfirma's en bellen je op. Er zou een probleem zijn met je computer en ze zullen het gratis oplossen...
Verbreek het contact met ongevraagde hulp of bel zelf via het officiële telnr van het bedrijf.
Ook helpdeskfraude van banken is populair. Ga nooit in op een voorstel om geld over te boeken op een andere rekening omdat uw rekening onregelmatigheden vertoont !

Microsoft

BIN Kenniscentrum Buurt.Informatie.Netwerk

Politie

Gouverneur Provincie Antwerpen Cathy Berx

provincie gouverneur Vlaams-Brabant

KORTRIJK

TIP
9

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

Stel je privacy-instelling zo hoog mogelijk in op **sociale media**. Alles wat je plaatst kan ge(mis)bruikt worden.

TIP
10

10 TIPS

VEILIGHEID in de digitale wereld is van cruciaal belang

Maak alleen verbinding met vertrouwde wifinetwerken, liefst geen publieke wifinetwerken

BIN Kenniscentrum Buurt.Informatie.Netwerk
Politie
Gouverneur Provincie Antwerpen Cathy Berx
provincie gouverneur Vlaams-Brabant
KORTRIJK

TIP
10

10 TIPS

1. Krijg je de juiste **inlogschermen** te zien?
Bij veel wifi-netwerken krijg je vooraf een inlogscherm te zien. Denk bijvoorbeeld aan ‘Wifi in de trein’ van NS. Voordat je dat netwerk gebruikt, moet je eerst je akkoord geven. Ook wifi in hotels of winkelcentra heeft vaak zo’n inlogpagina. Krijg je de pagina niet te zien terwijl je hem wel verwacht, dan heb je mogelijk te maken met iemand die zich voordoet als zo’n gratis netwerk. Zorg dan dat je dit netwerk vermijdt.

2. Gebruik alleen **mobiel internet**, download vooraf de data die je wil gebruiken (spotify, google maps...)
Heb je moeite met het onderscheiden van veilige en onveilige netwerken? Dan kun je gratis netwerken het beste helemaal vermijden. Bij de meeste abonnementen krijg je vaak een grote mobiele databundel, waarmee je aardig uit de voeten kunt. Bovendien is mobiel internet via 4G of 5G op de meeste plekken sneller dan wifi.

3. Gebruik eventueel een **VPN**
Om gevoelige informatie af te schermen van kwaadwillige personen, kun je ook een VPN gebruiken. VPN staat voor Virtual Private Network en versleutelt en anonimiseert je verkeer. Zo worden pottenkijkers buiten de deur gehouden. Hoewel een VPN instellen iets meer moeite kost, zorgt het wel voor behoorlijk wat extra zekerheid. *(Zowel IoS, Android als MS geven duidelijk richtlijnen voor het installeren van een VPN versleuteling)*

TIP 1 Gebruik complexe wachtwoorden

TIP 2 Kies voor tweestapverificatie

TIP 3 Zorg voor de software updates

TIP 4 Installeer een antivirusprogramma

TIP 5 Kijk uit voor verdachte berichten

TIP 6 APPS enkel via officiële bronnen

TIP 7 Klopt het website-adres ? Controle !

TIP 8 Let op voor dubieuze helpdeskmedewerkers

TIP 9 Controleer je privacy-instelling

TIP 10 Openbare WiFi-netwerken, Let op !

AANGIFTE

- Doe direct aangifte bij de politie wanneer u slachtoffer bent: time is of the essence (zonder aangifte is er geen onderzoek en kan je niet de schade verhalen)
- Verzamel zo veel mogelijk bewijs: correspondentie, (originele) e-mails, datum en tijdstippen, rekeningafschriften, profielen,…

- Wil je online een afspraak maken: https://www.politie.be/nl/

- Wil je online een aangifte doen, kan dat via: POLICE ON WEB www.police-on-web.be

SafeOnWeb

- Stuur een phishingbericht door naar verdacht@safeonweb.be.
- Ook verdachte SMS'jes kunnen hiernaar doorgestuurd worden

- Zij controleren de links en bijlages van deze berichten.
- Verdachte links laten zij blokkeren.

Bron: SafeOnWeb: https://www.safeonweb.be/nl

Miljoenen valse sms'jes geblokkeerd door telecomoperatoren

28 feb 2024

Heb jij ook het gevoel dat je nog maar weinig rare sms'jes krijgt? Tot voor kort deden verschrikkelijk veel vervelende sms'jes de ronde, maar sinds november van vorig jaar houden Telenet en Proximus verdachte sms-berichten systematisch tegen. Proximus alleen al kon 16 miljoen berichtjes van oplichters stoppen, kondigt Petra De Sutter, minister van Telecommunicatie aan.

Iedereen kent ze wel, die vervelende sms'jes die je te pas en te onpas krijgt en die vele mensen doen twijfelen.

Mama, dit is mijn nieuwe gsm-nummer. Je kan het oude nummer verwijderen.

Er wacht een pakje op jou! Klik hier om je pakje te volgen.

De bedoeling van deze berichtjes is eenvoudig: je op een link laten klikken en je gegevens opvragen, of botweg je vertrouwen wekken zodat je geld overmaakt aan oplichters. Precies deze berichtjes worden sinds enkele maanden gedetecteerd en geblokkeerd.

Proximus en Telenet doen daarvoor beroep op een nieuw platform dat door onder meer patroonherkenning verdachte sms'jes kan detecteren. Dit platform kwam tot stand onder impuls van minister De Sutter en als onderdeel van het nationale relanceplan. Het zogenaamd 'Stop Smishing project' is een samenwerking tussen het Centrum voor Cybersecurity België (CCB), het BIPT en de telecomoperatoren onder de verantwoordelijkheid van de minister van Telecommunicatie.

Het einde van phishing in zicht?

Na het succes van Stop Smishing wordt in een volgende stap gewerkt aan het tegenhouden van phishingberichten. Phishing is mogelijks nog een groter probleem dan smishing. Dagelijks sturen alerte burgers tot 30.000 verdachte berichten door naar verdacht@safeonweb.be. In 2023 ontvingen wij maar liefst 10 miljoen van dergelijke berichten, die tot grote ergernis van de internetgebruiker blijven de ronde doen.

Telecomoperatoren leggen zich steeds meer toe op het beveiligen van de e-mailaccounts van hun klanten. Onder meer via artificiële intelligentie zullen verdachte e-mails in de toekomst gedetecteerd en geblokkeerd worden. Het project zit nu in een proeffase, maar de vooruitzichten zijn veelbelovend.

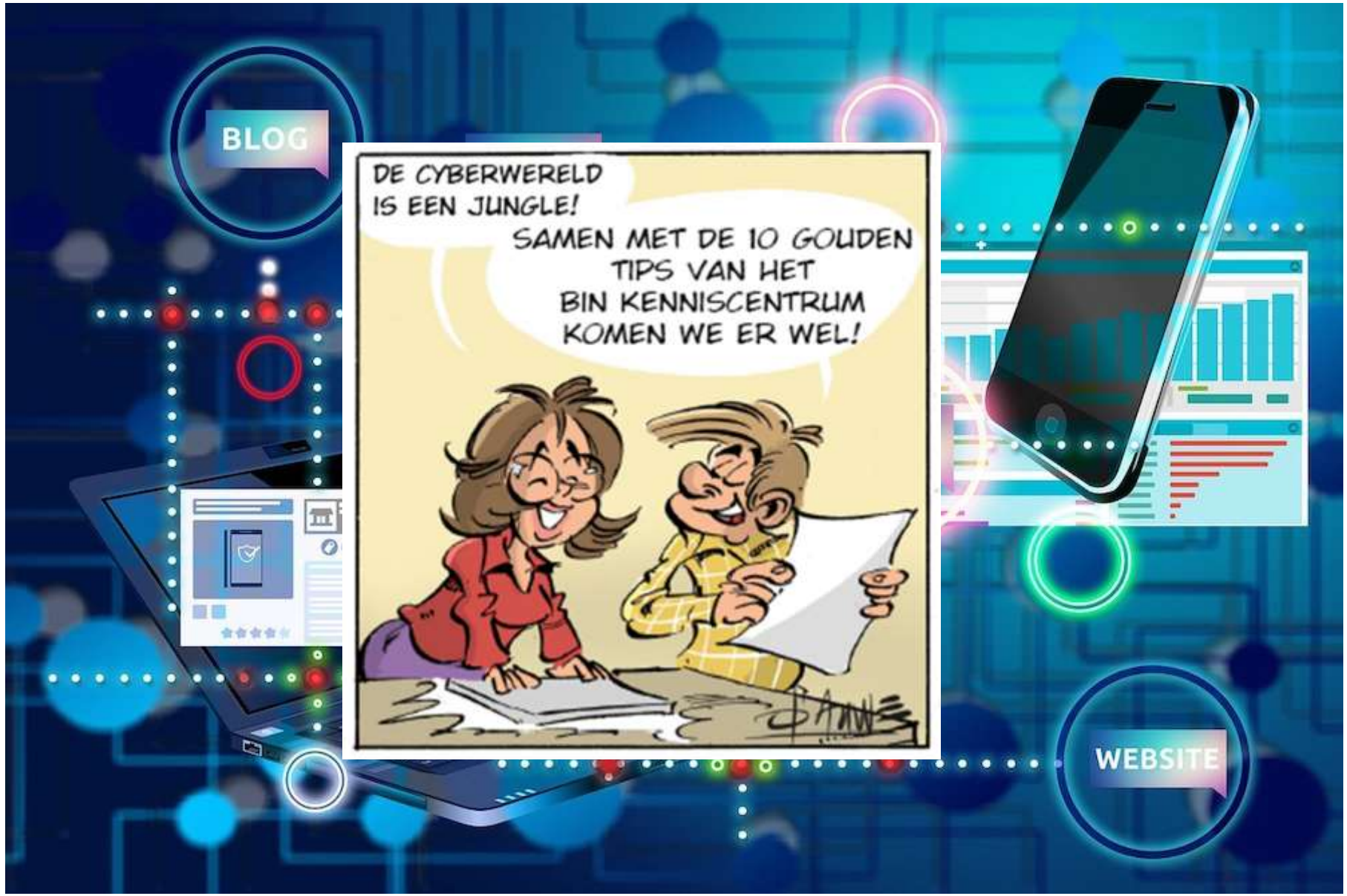
BIN Kenniscentrum Buurt.Informatie.Netwerk

Politie

Gouverneur Provincie Antwerpen Cathy Berx

provincie gouverneur Vlaams-Brabant

KORTRIJK


BLOG
DE CYBERWERELD IS EEN JUNGLE!
SAMEN MET DE 10 GOUDEN TIPS VAN HET BIN KENNISCENTRUM KOMEN WE ER WEL!
WEBSITE