

16 tips voor online veiligheid 01

Dit jaar neemt het aantal online apparaten wereldwijd toe tot meer dan 20 miljard. Dit zijn heel veel smartphones en computers, maar ook steeds meer alledaagse apparaten zoals koelkasten, wasmachines, smartwatches en zonnepanelen. Ook zelf zijn we steeds meer 'altijd verbonden' en daarmee ook 'altijd kwetsbaar'. Want gebruik van internet is niet zonder risico's.

Wat is er nodig om veilig online te kunnen zijn?

Tip 1 Het risico verlagen

In de echte wereld weten we wel hoe we het risico verlagen dat er schade ontstaat, bij digitale dreigingen is dat niet altijd zo duidelijk. De dreiging is vaak technisch en complex, de maatregel kost geld of beperkt het gebruiksgemak.

Een belangrijke maatregel die niets kost, is gezond wantrouwen. Een leuke site met gratis软件下载 kan gewoon een leuke site zijn, maar is het aannemelijk? Alleen gezond wantrouwen is helaas niet genoeg, daarvoor zijn de dreigingen groot en vaak ook onzichtbaar.

Gelukkig is er een breed aanbod aan beveiligingstools die de belangrijkste bedreigingen en de grootste risico's afdekken

Tip 2 Verschillende maatregelen

Beveiligingsmaatregelen kunnen op verschillende manieren worden onderverdeeld. Bijvoorbeeld naar de soort maatregel: proactief, detectief, reactief, correctief, preventief, compenserend, afsluitend en administratief.

Voor thuis zijn vooral de eerste vijf categorieën belangrijk. Proactieve maatregelen zijn gericht op het voorkomen van schade. Denk aan het installeren van updates en het beveiligen van gebruikersaccounts met multifactor-authenticatie. Detectieve maatregelen zijn gericht op het tijdig herkennen van een aanval. Bijvoorbeeld het controleren van logboeken.

Reactieve maatregelen moeten de schade beperken, zoals het maken van back-ups. Correctieve maatregelen lijken op reactieve, maar leggen meer nadruk op herstel en verbetering van de beveiliging daarna. Tot slot de preventieve maatregelen, die proberen vooral de impact van kwetsbaarheden te verminderen.

Denk aan het versleutelen van gegevens op een mobiele ssd en het verwijderen van niet-gebruikte software. In het algemeen geldt dat de bescherming beter is als uit meerdere categorieën maatregelen zijn genomen.

16 tips voor online veiligheid 02

Dit jaar neemt het aantal online apparaten wereldwijd toe tot meer dan 20 miljard. Dit zijn heel veel smartphones en computers, maar ook steeds meer alledaagse apparaten zoals koelkasten, wasmachines, smartwatches en zonnepanelen. Ook zelf zijn we steeds meer 'altijd verbonden' en daarmee ook 'altijd kwetsbaar'. Want gebruik van internet is niet zonder risico's.

Wat is er nodig om veilig online te kunnen zijn?

Tip 3 Vertrouw niemand

Gezond wantrouwen is een belangrijke stap in de beveiliging. Security-professionals hanteren als uitgangspunt 'zero trust' of vertaald 'nul vertrouwen'. Zij gaan er in hun werk vanuit dat geen enkel netwerk, apparaat en gebruiker volledig vertrouwd kan worden. Zero trust werd in 2010 geïntroduceerd door cybersecurityexpert John Lindervag, die ervoor pleitte beveiliging te bouwen vanuit de basis gedachte: never trust, always verify (nooit vertrouwen, altijd controleren).

Praktisch betekent dit: vaker controle van de identiteit van de mensen en apparaten in het netwerk, minimale toegang tot gegevens, minimale rechten op apparaten, en altijd denken dat de kwaadwillenden al binnen zijn in je netwerk. Zorg dus altijd voor aanvullende maatregelen, zoals het opdelen van een netwerk. Door op deze manier naar hun netwerk, gebruikers en apparaten te kijken, wordt het geheel sterker

Tip 4 Antiransomware, antimalware, antivirus

Hoewel het lastig is een ransomware-aanval helemaal te voorkomen, zijn er wel degelijk maatregelen die je kunt nemen. Gebruik van antivirussoftware is een belangrijke, zeker op een Windowspc.

Dit kan Windows Defender zijn, dat in de tests van gerenommeerde test-laboratoria AV-Test en AV-Comparatives doorgaans even goed als tot iets minder dan andere producten scoort. Het voordeel is dat het gratis is en prima integreert met andere beveiligingsmaatregelen in Windows.

Ook biedt het inmiddels extra bescherming tegen ransomware, doordat je bepaalde mappen, bestanden en delen van het geheugen tegen onbevoegde wijzigingen kunt beschermen.

16 tips voor online veiligheid 03

Dit jaar neemt het aantal online apparaten wereldwijd toe tot meer dan 20 miljard. Dit zijn heel veel smartphones en computers, maar ook steeds meer alledaagse apparaten zoals koelkasten, wasmachines, smartwatches en zonnepanelen. Ook zelf zijn we steeds meer 'altijd verbonden' en daarmee ook 'altijd kwetsbaar'. Want gebruik van internet is niet zonder risico's.

Wat is er nodig om veilig online te kunnen zijn?

Tip 5 Andere virusscanners

Gebruik van een alternatief antiviruspakket heeft een aantal voordelen vergeleken met Windows Defender. Het biedt, afhankelijk van de gekozen versie, meer beveiligingsfuncties en soms ook aanbeveiliging verwante functionaliteit.

Steeds meer antivirus- aanbieders bieden bovendien volwaardige ondersteuning aan consumenten. Dit is extra waardevol, juist omdat de consument anders dan bedrijven altijd minder ervaring en kennis met securityincidenten hebben dan bedrijven. De antivirus levert dan die kennis en 'handjes'

Tip 6 Extra beveiliging

In de eerdere antivirustesten bleek al dat beschermingsproducten van Bitdefender, F-Secure, ESET en McAfee goed scoorden op bescherming tegen phishing en van de identiteit, als aanvulling op Windows Defender.

Ook beveiligen ze meer dan alleen je Windowscomputer, bijvoorbeeld mobiele apparaten, en de verschillende desktops en notebooks van Apple. Bovendien hoeft dit niet te betekenen dat je Windows defender verliest.

Dat kan ook bestaan naast een andere beveiligingsoplossing en regelmatig een extra scan doen. Klik hiervoor op **Start / Systeem / Privacy en beveiliging / Virus- en bedreigingsbeveiliging**

Tip 7 Decryptors

Ben je ondanks alle voorzorg toch geraakt door ransomware? De site www.nomoreransom.org (een samenwerking van Europol, Politie, Kaspersky, McAfee en veel andere securityorganisaties) biedt gratis hulp.

Behalve adviezen om ransomware te voorkomen, zijn er voor diverse ransomware-varianten gratis decryptors te downloaden. Daarmee kun je zonder te betalen de ransomware-versleuteling ongedaan maken.

16 tips voor online veiligheid 04

Dit jaar neemt het aantal online apparaten wereldwijd toe tot meer dan 20 miljard. Dit zijn heel veel smartphones en computers, maar ook steeds meer alledaagse apparaten zoals koelkasten, wasmachines, smartwatches en zonnepanelen. Ook zelf zijn we steeds meer 'altijd verbonden' en daarmee ook 'altijd kwetsbaar'. Want gebruik van internet is niet zonder risico's.

Wat is er nodig om veilig online te kunnen zijn?

Tip 8 Back-up

Antimalware-beveiliging verlaagt het risico op een succesvolle ransomware-aanval, maar er zijn aanvullende maatregelen mogelijk om het risico verder te verkleinen. Een heel belangrijke is het regelmatig back-uppen van de belangrijkste gegevens. Windows biedt wel een back-upfunctie, maar die werkt alleen met een Windows-account en cloudopslag op OneDrive. Duplicati (www.duplicati.com) is een gratis alternatief, dat tal van back-uplocaties ondersteunt. Acronis True Image (www.acronis.com) biedt ook antivirus en cloudopslag, maar wel in een jaarabonnement.

De back-ups moeten daarbij zeker niet op hetzelfde apparaat staan als de gegevens die in de back-up zitten. Beter worden de back-ups op een ander apparaat bewaard en het liefst offline. Dat betekent op een externe schijf of in de cloud. Alleen een back-up die niet toegankelijk is voor buitenstaanders, is immers veilig voor ransomware

Tip 9 Gebruik een NAS

Een NAS is een prima apparaat als onderdeel van een back-upstrategie, maar kan nooit het enige onderdeel in die strategie zijn. Een NAS is veelal permanent ingeschakeld en de back-ups opgeslagen op de NAS zijn dan ook bereikbaar via het netwerk, dus ook door eventuele malware.

Daarbij heeft Synology, maar vooral QNAP, een historie van kwetsbaarheden in de NAS-software en geven beide pas recent echt aandacht aan beveiliging. Omdat het niet is uit te sluiten dat de ransomware besmetting in een van de back-ups zit, is het noodzakelijk voldoende versies van elke back-up te bewaren. En essentieel, de back-ups moeten worden getest.

Zonder regelmatige controle of de back-ups volledig en bruikbaar zijn, vormen ze geen zekerheid waar je op kunt vertrouwen als je ooit te maken krijgt met ransomware en je al je gegevens uit de back-up wilt herstellen in plaats van te betalen

16 tips voor online veiligheid 05

Dit jaar neemt het aantal online apparaten wereldwijd toe tot meer dan 20 miljard. Dit zijn heel veel smartphones en computers, maar ook steeds meer alledaagse apparaten zoals koelkasten, wasmachines, smartwatches en zonnepanelen. Ook zelf zijn we steeds meer 'altijd verbonden' en daarmee ook 'altijd kwetsbaar'. Want gebruik van internet is niet zonder risico's.

Wat is er nodig om veilig online te kunnen zijn?

Tip 10 Alles Up-to-date houden

Updates zijn essentieel voor de beveiliging van elk toestel. Telefoon, tablet, Mac, Windows-pc: installeer altijd alle updates. Android, iOS, macOS en Windows beschikken allemaal over functionaliteit om de software te updaten.

Installeer updates zo snel mogelijk en herstart indien gevraagd het systeem om vooral kritische updates ook echt actief te maken. Lastiger is het updaten van alle programma's die je als gebruiker er zelf op zet.

Ook die moeten bijgewerkt worden als er een nieuwe versie uitkomt, alleen ontbreekt de mogelijkheid dit eenvoudig te doen. Er zijn alternatieve programma's die zelf de geïnstalleerde programma's indexeren en scannen op achterlopende updates.

Naar aanleiding van een eerdere test adviseren we UnigetUI (www.github.com/marticliment/UniGetUI) en VulnDetect (www.secteer.com). UnigetUI werkt als een traditioneel Windows-programma, maar is eigenlijk een interface rond de niet-grafische updatemanager van Windows zelf, genaamd winget. UnigetUI heette oorspronkelijk WingetUI.

Die grafische interface maakt het gebruiksvriendelijk én zeer rijk aan functionaliteit. Eenvoudiger is VulnDetect, een dienst die nagenoeg onzichtbaar werkt. Alle configuratie en gebruik gaat via een webportal.

Voor thuisgebruikers is het tot vijf apparaten gratis. Beide programma's updaten nagenoeg alle geïnstalleerde software en bewaken ook zaken als browsers en Windows Updates.

16 tips voor online veiligheid 06

Dit jaar neemt het aantal online apparaten wereldwijd toe tot meer dan 20 miljard. Dit zijn heel veel smartphones en computers, maar ook steeds meer alledaagse apparaten zoals koelkasten, wasmachines, smartwatches en zonnepanelen. Ook zelf zijn we steeds meer 'altijd verbonden' en daarmee ook 'altijd kwetsbaar'. Want gebruik van internet is niet zonder risico's.

Wat is er nodig om veilig online te kunnen zijn?

Tip 11 Zichtbare beveiliging

Bij verlies dekt de verzekering mogelijk wel de financiële schade, maar een verzekeraar kan nooit voorkomen dat de dief zich toegang tot jouw gegevens op jouw laptop verschaft. Geen fijn gevoel.

Geef dieven geen kans. Het Kensington-slot is een standaarduitsparing in de behuizing van laptop of tablet die het mogelijk maakt deze met een kabel aan een verwarmingsbuis of ander object vast te leggen.

Dat geeft een gerust gevoel als je even koffie gaat halen. Reis je veel, overweeg dan een privacyscherm. Dit zet je voor het scherm van de laptop en voorkomt dat iedereen die naast je in vliegtuig of trein zit, kan meekijken. Het zijn eenvoudige maatregelen die de digitale veiligheid flink verbeteren.

Tip 12 Update je hardware

Niet alleen de software op de pc is kwetsbaar als het niet is geüpdatet naar de laatste versie, dit geldt ook voor alle apparaten in het thuisnetwerk. En dat zijn er steeds meer. Lang niet allemaal krijgen ze automatisch updates of zijn er überhaupt updates voor beschikbaar.

Door de veelheid aan merken en modellen is er helaas geen eenvoudige oplossing voor dit probleem. Een belangrijke stap is allereerst uitzoeken welke apparatuur er allemaal in het netwerk aanwezig is.

Hierbij kan een netwerkscanner helpen. Verschillende aanbieders van antivirusoplossingen bieden in hun apps voor mobiele apparaten zo'n functie

16 tips voor online veiligheid 07

Dit jaar neemt het aantal online apparaten wereldwijd toe tot meer dan 20 miljard. Dit zijn heel veel smartphones en computers, maar ook steeds meer alledaagse apparaten zoals koelkasten, wasmachines, smartwatches en zonnepanelen. Ook zelf zijn we steeds meer 'altijd verbonden' en daarmee ook 'altijd kwetsbaar'. Want gebruik van internet is niet zonder risico's.

Wat is er nodig om veilig online te kunnen zijn?

Tip 13 Netwerk scanner

Een andere optie is een losse netwerkscanner-tool. Een uitgebreide en gebruiksvriendelijke is Fing (www.fing.com), dat als app voor Windows, macOS, iOS en Android beschikbaar is, maar dat ook een Fing Agent voor installatie op een Raspberry Pi aanbiedt. Afhankelijk van de gebruikte versie en een eventueel abonnement, bewaakt Fing het hele netwerk, brengt alle apparaten in beeld en rapporteert ook over achterlopende versies.

Zijn de apparaten in beeld, dan moeten deze veelal stuk voor stuk handmatig bijgewerkt worden. Hiervoor log je met de browser in op elk apparaat en voer je een firmware-update of upgrade uit. Veelal kan dit direct op het apparaat, soms moet de firmware eerst gedownload worden naar een pc of Mac en van daar geüpload.

Belangrijk is ook hardware waarvoor geen updates meer uitkomen en waarbij lekken dus niet gedicht worden, uit het netwerk te halen en vervangen door nieuwe die nog wel door de leverancier ondersteund worden.

Tip 14 IoT en andere apparaten

Met up-to-date firmware leg je alleen de basis voor de verdere beveiliging van de apparaten in het net werk. Wat er aanvullend kan, verschilt per apparaat. Wat er moet, is wel helder. Geef alleen apparaten die dat nodig hebben toegang tot het internet. Verander waar mogelijk de naam van het admin-account en voorzie elk account van een per apparaat verschillend wachtwoord.

Maak als dat mogelijk is voor het gebruik een account aan zonder admin-rechten en gebruik dat voor bijvoorbeeld het bekijken van camerabeelden of het instellen van de kamertemperatuur. Schakel apparatuur die niet altijd nodig is ook uit op momenten dat het niet nodig is. Een NAS kan dit bijvoorbeeld volgens een vast schema. Deel het netwerk op in verschillende segmenten.

Bijna elke router biedt wel de mogelijkheid voor een gastnetwerk, maar soms kun je ook zelf meerdere netwerken aanmaken. Zet al deze minder betrouwbare apparaten in een eigen netwerk en geef ze alleen toegang tot internet. Of plaats apparaten die verbinding met het thuisnetwerk moeten hebben in een apart segment dat juist geen internettoegang heeft

16 tips voor online veiligheid 08

Dit jaar neemt het aantal online apparaten wereldwijd toe tot meer dan 20 miljard. Dit zijn heel veel smartphones en computers, maar ook steeds meer alledaagse apparaten zoals koelkasten, wasmachines, smartwatches en zonnepanelen. Ook zelf zijn we steeds meer 'altijd verbonden' en daarmee ook 'altijd kwetsbaar'. Want gebruik van internet is niet zonder risico's.

Wat is er nodig om veilig online te kunnen zijn?

Tip 15 Bescherm je identiteit

Omdat identiteitsfraude alsmat toeneemt en de schade groot kan zijn, is het belangrijk ook je eigen identiteit goed te beschermen. Zet accounts op social media van 'publiek' naar 'alleen toegankelijk voor vrienden', waarbij je contacten bewust moet toelaten. Schoon de lijst gerust ook eens op met contacten die geen vrienden meer zijn.

Verwijder accounts van onlinediensten die je niet meer gebruikt of voorzie ze van een enorm lastig wachtwoord dat je dan ook zelf niet eens hoeft te onthouden. Veel antivirussoftware biedt functionaliteit zoals anti-phishing, bescherming tegen malafide websites en controle op gelekte identiteits-informatie op het darkweb.

Voor de laatste analyseren zij datasets uit datalekken. Als alternatief kun je dit ook zelf controleren op Have i been pwned? www.haveibeenpwned.com , en daar voor een of meer mailadressen ook een alert instellen, zodat je melding krijgt als jouw gegevens worden gevonden

Tip 16 Extra authenticatie

De beveiliging van accounts neemt enorm toe wanneer je aan het wachtwoord een extra authenticatie toevoegt. Dat kan een unieke code zijn of het bevestigen van een login in een authenticatie-app zoals Google of Microsoft Authenticator. Het voordeel hiervan is dat het gratis is.

Het bezit van de smartphone en de toegangscontrole in die app zijn dan extra bewijs dat jij bent wie je zegt te zijn bij het inloggen. Het nadeel is dat de smartphone zelf gestolen kan worden of kan worden gehackt. Als alternatief kun je een hardware sleutel nemen. Die van Yubikey zijn de bekendste, maar er zijn meer merken die deze oplossing bieden.

De prijzen van deze sleutels lopen uiteen van 20 tot 80 euro. Belangrijk is vooraf goed te kijken waarvoor je ze wilt gebruiken en welke accounts een hardware sleutel ondersteunen. Voor gebruik in combinatie met een wachtwoordmanager zijn ze erg geschikt en bijna al de hele investering waard. Bedenk wel, één sleutel is eigenlijk geen sleutel; zorg altijd voor een back-up.