

5 Basic Online Safety Tips

A text message here, an email there. Sharing photos and videos on social media. Video calls with family and friends. Transferring money through Tikkie or your banking app. Accessing government services or medical appointments through DigiD. Wireless printing, remotely setting your home burglar alarm or putting on the heating... The internet makes daily life easier and more comfortable for so many people.

It is important to keep all your devices and accounts secure, from your smartphone to your printer, from Instagram to Gmail. Criminals are sadly just as active online as they are in the offline world. Take these five steps to secure your basic online safety. Make it that bit harder for cyber criminals.

01 - Set secure passwords for all your devices and accounts:



- The longer the better. Use a passphrase.
- Use a different password for each account. Keep your passwords in a password manager.
- Use two-factor authentication to log in where possible.

02 - Always update your smart devices immediately



- Smart devices are devices connected to the internet like printers, baby monitors, doorbells and even robot vacuum cleaners.
- Manufacturers keep your devices more secure with updates. So don't close those notifications!



03 - Use antivirus software

- Antivirus software scans your device for threats like viruses, malware and malicious apps.



04 - Back up your data regularly

- If hacked, you could lose everything. So make a copy of your files just in case.



05 - Always check before you click

- Criminals on the internet send fake links through emails, text messages or payment requests. They use these to get you to share your data or transfer money.

If you want to learn more about online safety, go to veiliginternetten.nl/5-tips-basisveiligheid

5 basistips voor je online veiligheid

Appje hier, e-mail daar. Foto's en video's delen via social media. Videobellen met vrienden en familie. Geld overmaken via een Tikkie of je bank-app. Inloggen bij de overheid of huisarts via DigiD. Draadloos printen, het alarm of de verwarming in huis instellen... Het internet maakt het dagelijks leven voor veel mensen een stuk leuker en makkelijker.

Het is belangrijk dat je al je apparaten en accounts goed beveiligt. Van je smartphone tot je printer, van Instagram tot Gmail. Want net als in de offlinewereld, zijn criminelen online helaas ook actief. Door deze vijf acties uit te voeren, zorg jij ervoor dat je online basisveiligheid op orde is. Zo maak je het cybercriminelen een stuk moeilijker.

01 - Zorg voor veilige wachtwoorden voor al je apparaten en accounts. Dat betekent:

- Hoe langer, hoe beter. Gebruik een wachtwoordzin.
- Gebruik voor elk account een ander wachtwoord. En bewaar je wachtwoorden in een wachtwoordmanager.
- Gebruik waar het kan inloggen in twee stappen.

02 - Doe altijd direct software updates van je slimme apparaten



- Een slim apparaat is een apparaat dat met het internet verbonden is. Zoals sommige printers, babyfoons en deurbellen. Maar ook een robotstofzuiger.
- Met updates zorgen fabrikanten dat de beveiliging van je apparaten altijd op orde is. Klik die pop-ups dus niet weg!



03 - Gebruik een virusscanner

- Een virusscanner controleert je apparaat op allerlei narigheid, zoals virussen, malware, en kwaadaardige apps.



04 - Maak regelmatig een back-up

- Als je gehackt wordt, kan je alles kwijt zijn. Maak daarom een kopie van je bestanden, voor de zekerheid.



05 - Eerst checken, dan klikken

- Internetcriminelen versturen via een e-mail, tekstbericht of betaalverzoek valse linkjes. Zo proberen ze je over te halen om gegevens te delen of geld over te maken.

Meer weten over online basisveiligheid? Ga naar veiliginternetten.nl/5-tips-basisveiligheid

5 conseils de base pour votre sécurité en ligne

Une appli ici, un e-mail là. Partager des photos et des vidéos sur les réseaux sociaux. Faire des appels visio avec les amis et la famille. Transférer de l'argent par Tikkie ou l'appli de votre banque. Se connecter sur un site du gouvernement ou le site de votre médecin généraliste par DigiD. Imprimer sans fil, régler l'alarme ou le chauffage chez soi... Internet rend la vie nettement plus agréable et plus simple à beaucoup de personnes.

Il est important que vous protégez bien tous vos appareils et vos comptes. De votre smartphone à votre imprimante, d'Instagram à Gmail. En effet, comme dans le monde physique, des criminels œuvrent malheureusement en ligne. En exécutant ces cinq actions, vous assurerez votre sécurité de base en ligne. Ainsi, vous rendrez la vie nettement plus compliquée aux cybercriminels.

01 - Veillez à disposer de mots de passe sûrs pour tous vos appareils et comptes. Voici les règles à appliquer :

- Plus le mot de passe est long, mieux c'est. Utilisez une phrase secrète.
- Utilisez un mot de passe différent pour chaque compte. Et conservez vos mots de passe dans un gestionnaire de mots de passe.
- Lorsque c'est possible, connectez-vous en deux étapes.

02 - Mettez toujours immédiatement à jour les logiciels de vos appareils connectés



- Un appareil connecté est un appareil qui est connecté à Internet, comme certaines imprimantes, certains babyphones et certaines sonnettes de portes, mais aussi un aspirateur robot.
- Les mises à jour permettent au fabricant de veiller à la sécurité permanente de vos appareils. Alors ne fermez pas les pop-ups !

03 - Utilisez un scanner antivirus



- Un scanner antivirus vérifie l'absence de toutes sortes de désagréments sur votre appareil, comme des virus, des logiciels et des applis malveillants.

04 - Réalisez des back-up réguliers



- Si vous vous faites pirater, vous pouvez tout perdre. Par conséquent, effectuez une copie de vos fichiers par sécurité.

05 - Vérifier d'abord, cliquer ensuite



- Les cybercriminels envoient de faux liens par e-mail, SMS ou demande de paiement. Ils essaient ainsi de vous convaincre de partager des données ou de transférer de l'argent.

Vous voulez en savoir plus sur la sécurité de base en ligne ? Rendez-vous sur la page veiliginternetten.nl/5-tips-basisveiligheid (en néerlandais)

5 основних порад для вашої безпеки онлайн

Купа застосунків та повідомлень. Надсилення фотографій та відеороликів через соцмережі. Відеодзвінки друзям і родичам. Переказ грошей через Tikkie чи банківський застосунок. Реєстрація в органах влади чи запис до лікаря через DigiD. Бездротовий друк, налаштування сигналізації чи опалення в будинку... Інтернет робить повсякденне життя набагато веселішим і простішим для багатьох людей.

І дуже важливо належним чином захистити всі свої пристрої та облікові записи. Це стосується всього: від смартфона до принтера, від Instagram до Gmail. Тому що так само, як і в реальному світі, злочинці, на жаль, активні також в Інтернеті. Дотримуючись цих п'яти порад, ви забезпечите свою базову безпеку онлайн. Таким чином, ви значно ускладните життя кіберзлочинцям.

01 - Встановіть надійні паролі для всіх своїх пристроїв та облікових записів. Це означає:

- Чим довше, тим краще. Використовуйте ключову фразу.
- Використовуйте різні паролі для кожного облікового запису. І зберігайте свої паролі в менеджері паролів.
- За можливості використовуйте двофакторну автентифікацію.

02 - Завжди оновлюйте програмне забезпечення на своїх «розумних» пристроях



- «Розумний» пристрій — це той, що підключений до мережі Інтернет. Це можуть бути деякі принтери, радіоняні та дверні дзвінки. І навіть робот-пилосос.
- За допомогою оновлень виробники гарантують, що безпека ваших пристроїв залишатиметься на належному рівні. Тож не закривайте одразу ці спливаючі сповіщення про оновлення!

03 - Використовуйте антивірусну програму



- Антивірус перевіряє ваш пристрій на наявність різного роду небезпек, таких як віруси, шкідливе програмне забезпечення та небезпечні застосунки.

04 - Регулярно створюйте резервні копії



- Якщо вас зламають, ви можете втратити все. Тому задля впевненості робіть копії своїх файлів.

05 - Спочатку перевіряйте, а потім натискайте



- Інтернет-злочинці надсилають фальшиві посилання через електронну пошту, текстові повідомлення чи платіжні вимоги. Так вони намагаються переконати вас поділитися даними чи переказати гроші.

Хочете дізнатися більше про основи безпеки в Інтернеті? Переходьте за посиланням veiliginternetten.nl/5-tips-basisveiligheid

5 podstawowych wskazówek dla Twojego bezpieczeństwa online

Tutaj apka, tam e-mail. Publikowanie zdjęć i filmów w mediach społecznościowych. Wideorozmowy z przyjaciółmi i rodziną. Przesyłanie pieniędzy za pośrednictwem Tikkie lub aplikacji bankowej. Logowanie się na stronach urzędów lub przychodni za pomocą DigiD. Drukowanie bezprzewodowe, sterowanie alarmem lub ogrzewaniem w domu... Internet sprawia, że codzienne życie wielu osób staje się nieco przyjemniejsze i łatwiejsze.

Ważnym jest, by dobrze zabezpieczać wszystkie swoje urządzenia i konta. Od smartfonu po drukarkę i od Instagrama po Gmail. Gdyż podobnie jak w świecie poza siecią, również w Internecie przestępcy niestety nie próżnują. Wykonując tych pięć działań, zadbasz o prawidłowe, podstawowe bezpieczeństwo w sieci. Utrudnisz w ten sposób działanie cyberprzestępcom.

01 - Dbaj o stosowanie bezpiecznych haseł na wszystkich swoich urządzeniach i kontach. Oznacza to:

- Im dłuższe hasło, tym lepsze. Użyj hasła w postaci zdania.
- Używaj innego hasła dla każdego konta. Przechowuj swoje hasła w menedżerze haseł.
- Tam, gdzie to możliwe, korzystaj z logowania dwuetapowego.

02 - Zawsze od razu aktualizuj oprogramowanie swoich urządzeń smart



- Urządzenie smart to takie, które jest podłączone do Internetu. Może to być drukarka, niania elektroniczna czy domofon. Ale także odkurzacz automatyczny.
- Poprzez aktualizacje producenci dbają o to, by urządzenia były przez cały czas zabezpieczone. Nie zamykaj zatem okienek z prośbą o aktualizację!



03 - Używaj skanera wirusów

- Skaner wirusów kontroluje Twoje urządzenie pod kątem jakichkolwiek problemów, takich jak wirusy, złośliwe oprogramowanie czy niebezpieczne aplikacje.



04 - Regularnie wykonuj kopie zapasowe

- W razie zhakowania możesz stracić wszystko. Dlatego też dla pewności wykonuj kopie swoich plików.

05 - Najpierw sprawdź, potem klikaj

- Cyberprzestępcy wysyłają fałszywe linki za pośrednictwem e-maili, wiadomości tekstowych czy próśb o dokonanie zapłaty. W ten sposób próbują nakłonić Cię do udostępnienia im danych lub przekazania pieniędzy.

Chcesz dowiedzieć się więcej na temat bezpieczeństwa w sieci? Wejdź na stronę [veiliginternetten.nl/5-tips-basisveiligheid](https://www.veiliginternetten.nl/5-tips-basisveiligheid)

5 نصائح أساسية للبقاء آمنًا ومستمتعًا أثناء وجودك في عالم الإنترنت

الإنترنت، هذا العالم المتصل الذي يمتد إلى كل ركن من أركان حياتنا، حيث يُمنحنا مجموعة واسعة من التطبيقات والتقنيات التي تجعل الحياة أسهل وأكثر متعة. فيتيح لنا التواصل الفعّال عبر الرسائل الإلكترونية. إلى جانب مشاركة اللحظات المميزة عبر الصور والفيديوهات على منصات التواصل الاجتماعي، والاتصالات المرئية مع الأحباء والأصدقاء. كما يُتيح لنا إتمام المعاملات المالية عبر تطبيقات مثل تيكّي أو التطبيقات المصرفية، وكذلك الوصول إلى الخدمات الحكومية أو استشارات الطبيب عبر الهوية الرقمية. حتى الأمور اليومية مثل الطباعة اللاسلكية وضبط أنظمة الإنذار والتدفئة وغيرها تتم بسهولة ويُسر عبر الإنترنت. هذا العالم الافتراضي يُضفي لمسات من السهولة والمتعة على حياتنا، ويجعل الأنشطة اليومية سلسلة وممتعة للكثيرين.

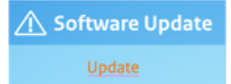
ومع سعينا نحو السلامة الرقمية، يجب أن نؤكد على حماية كافة أجهزتنا وحساباتنا الرقمية. من الهواتف الذكية إلى الطابعات، وكل تطبيقاتنا الرقمية. فعلى غرار العالم الحقيقي، يترصد بنا المجرمون والمحتالون أيضًا في زوايا الإنترنت. هنا، سنقدم لك خمس نصائح أساسية لتعزيز أمانك وسلامتك أثناء تواجدك على الإنترنت. ستسهم هذه النصائح في تعقيد مهمة المجرمين الإلكترونيين وصعوبة التسلل والتلاعب بأمانك الرقمي.

1 - تأكد من وجود كلمات مرور آمنة لجميع أجهزتك وحساباتك. وذلك عن طريق اتباع الخطوات التالية:

- قم باختيار كلمات مرور طويلة، فكلما طالت كلمة المرور كان ذلك أفضل. ويُفضل صياغة كلمات المرور باستخدام جمل كاملة.
- استخدم كلمة مرور مختلفة لكل حساب، واحفظ هذه الكلمات في مدير كلمات المرور.
- استخدم آلية التحقق الثنائي لتسجيل الدخول حيثما أمكن ذلك.

2 - لا تُهمل أبدًا تحديثات البرامج على أجهزتك الذكية فور توفرها

- الجهاز الذكي هو الذي يتصل بالإنترنت. مثل بعض الطابعات وكاميرات مراقبة الأطفال وأجراس الباب، وحتى المكينة الكهربائية الروبوتية تعتبر جهازًا ذكيًا.
- من خلال تلك التحديثات، تكفل الشركات المصنّعة دائمًا سلامة أجهزتك. لذا، لا تتجاهل هذه النوافذ المنبثقة!



3 - احرص على استخدام برامج مضادة للفيروسات

- هذه البرامج تقوم بفحص جهازك لاكتشاف جميع أنواع البرامج الضارة مثل الفيروسات، والبرمجيات الخبيثة، والتطبيقات الضارة.



4 - حافظ على إنشاء نسخ احتياطية بشكل منتظم

- في حالة اختراق جهازك، يمكن أن تخسر كل شيء. لذا، احرص على عمل نسخ احتياطية لملفاتك كإجراء احترازي.



5 - كن حذرًا وتحقق قبل النقر

- يُرسل المحتالون روابط مزيفة عبر البريد الإلكتروني أو الرسائل النصية أو طلبات الدفع. وذلك بهدف إقناعك بمشاركة بياناتك أو تحويل الأموال.



للمزيد من المعلومات حول وسائل السلامة الأساسية عبر الإنترنت، تفضل بزيارة
veiliginternetten.nl/5-tips-basisveiligheid

نحن هنا للإجابة على الأسئلة وتقديم المساعدة في حال وجود أي مشكلة. هذه الخدمة متاحة للجميع.

www.veiliginternetten.nl | info@veiliginternetten.nl

5 consejos básicos para tu seguridad online

App por aquí, correo electrónico por allá. Compartir fotos y vídeos en redes sociales. Videollamadas con amigos y familiares. Transferir dinero mediante Tikkie o la app de tu banco. Iniciar sesión en la administración pública o en el médico de familia mediante DigiD. Imprimir sin cables, ajustar la alarma o la calefacción de casa... Internet hace que la vida diaria de muchas personas sea un poco más divertida y sencilla.

No obstante, es fundamental proteger adecuadamente todos tus dispositivos y cuentas. Desde tu teléfono inteligente hasta tu impresora, desde Instagram hasta Gmail. Porque, al igual que en el mundo real, los delincuentes también están activos en la red. Aplicando estas cinco medidas, garantizarás tu correcta seguridad básica en línea. De esta forma se lo pones mucho más difícil a los ciberdelincuentes.

01 - Asegúrate de establecer contraseñas seguras para todos tus dispositivos y cuentas. Cómo se hace:

- Cuanto más larga sea, mejor. Utiliza una frase de contraseña.
- Utiliza una contraseña distinta para cada cuenta. Y guarda tus contraseñas en un gestor de contraseñas.
- Utiliza un inicio de sesión en dos pasos allí donde se te permita hacerlo.

02 - Actualiza siempre enseguida el software de tus dispositivos inteligentes



- Un dispositivo inteligente es un dispositivo que está conectado a Internet, como algunas impresoras, teléfonos y timbres de la puerta, o también muchos robots aspiradores.
- Con las actualizaciones, los fabricantes se aseguran de que la seguridad de los aparatos siempre esté garantizada. Por lo tanto, ¡no cierres esas ventanas de actualización que te aparecen!



03 - Usa un antivirus

- Un antivirus examina tu dispositivo en busca de todo tipo de problemas, como virus, malware y apps maliciosas.

04 - Haz copias de seguridad con regularidad

- Si te hackean, podrías perderlo todo. Por eso te recomendamos hacer una copia de tus archivos, por si acaso.



05 - Asegúrate primero antes de hacer clic

- Los ciberdelincuentes envían enlaces maliciosos en correos electrónicos, mensajes de texto o solicitudes de pago falsos. Con ellos intentan persuadirte para que compartas tus datos o les transfieras dinero.

¿Quieres obtener más información sobre la seguridad básica online?
Consulta [veiliginternetten.nl/5-tips-basisveiligheid](https://www.veiliginternetten.nl/5-tips-basisveiligheid)

5 n nnsa'iḥ asasiyya i raman di internet

Ijjen tebraṭ da ḍ ijjen e-mail diha. Apartaj n ṭsawar ḍ yidyawaṭ di ssocial medya. Yamadaṭ n yidyu ak familya ḍ imeḍḍukar. Asekki n tmenyaṭ s Tikkie niḃ s l'App n rbanku ennec/ennem. Awaḍ ya lxadamaṭ n lḥukuma niḃ arrundiyyu/sita s DigiD. Adbaε bra ikabliten, areglar n alarma n iceffan di taḍḍaṭ ennec/ennem zi ragwaj niḃ asexdem n klima...Internet itarra tudarṭ n bnaḍem n kur nhar tesher u muriḥa i aṭṭas n iwdan.

Muhim s waṭṭas aṭḥafdeḍ x raman n iparatuten d reḥsabaṭ ennec/ennem di raman, zi ṭṭilifun ennec/ennem ar macina n wedbaε ennec/ennem, zi Instagram ar Gmail. Iteqqes rḥar rami lmujrimin necten di internet am mamec necten barra i internet. Ksi 5 n nnsa'iḥa-ya ḥenja atsiyuraḍ raman ennec/ennem l'asasi di internet. Seqseḥ manayenni x lmujrimin n internet.

01 - Eg kudaṭ qes-ḥen di mmarra iparatuten ḍ reḥsabaṭ ennec/ennem:

- Kurma dazirar, kurma ḥsen. Eg ijjen lεibara n ssir.
- Eg ijjen lkuḍ mextalef i kur reḥsab. Xemmer lkudaṭ ennec/ennem deg-ijjen App n uxemmer n lkudaṭ.
- Sexdem lmusadaqa ṭṭuna'iyya ḥenja atsejleḍ adaf ennec/ennem kurma ṭzemmaḍ.



02 - Eg rebda ṭṭeḥdiṭ i iparatuten "smart" ennec/ennem deyya

- Iparatuten "smart" ḍ iparatuten kunektan ya internet am macinat n weḍbaε, pantayaṭ n iḥḍiden, ssunit n tiwwura ḍ timedwasin n tfawṭ.
- Fabrikaṭ ṭḥafadent x raman n iparatuten ennec/ennem s ṭṭaḥḍitaṭ. X manayenni wa ṭṭeqqen-ca nutifikasyunaṭ enni!



03 - Sexdem prugramaṭ n antiyirus

- Prugramaṭ n antiyirus teskanan aparatu ennec/ennem ḥenja adazun x ṭṭaḥḍitaṭ am lyirusaṭ, prugramaṭ i ḍḍarran.



04 - Eg kupya i lbayanaṭ ennec/ennem kur amar

- Mara hakanc/hakancem, ṭzemmaḍ atexsaḍ kurci. U x manayenni, eg ijjen kupya i lmileffaṭ ennec/ennem ḥenja ateqqimeḍ trankil.

05 - Rebda ṭḥeqqaq zi rḥajeṭ i xef ya tεebzeḍ qber ma xas tεebzeḍ

- Lmujrimin di internet ssekan l-linkat mzewrin s e-mail, tibratin niḃ ṭṭalabat n uxeḍḍes. ṭṭeggen manayenni ḥenja asen tewced lmeεlumat ennec niḃ ḥenja asen tessekkeḍ tmenyaṭ.

Mara tesseḍ atesneḍ ktar x raman di internet, ruḥ ya veiliginternetten.nl/5-tips-basisveiligheid

Çevrimiçi güvenliğiniz için 5 temel öneri

Uygulamalar, e-postalar... Sosyal medyada fotoğraflar ve video paylaşmak. Arkadaşlarla ve aileyle görüntülü görüşmek. Tikkie veya banka uygulamaları üzerinden para göndermek. DigiD üzerinden devlet veya aile doktoru platformlarında oturum açmak. Kablosuz bağlantıyla belge yazdırmak veya evinizin ısıtma sistemini ayarlamak... İnternet, birçok kişinin günlük hayatını daha keyifli ve kolay bir hâle getiriyor.

Tüm cihazlarınızın ve hesaplarınızın güvenliğini sağlamanız çok önemli. Akıllı telefonunuzdan yazıcınıza, Instagram'dan Gmail'e... Çünkü tıpkı çevrimdışı hayatımızda olduğu gibi ne yazık ki çevrimiçi ortamda da suçlular boş durmuyor. Bahsedeceğimiz bu beş önlemi alarak temel çevrimiçi güvenliğinizi sağlayabilirsiniz. Böylece siber suçluların işini zorlaştırabilirsiniz.

01 - Bütün cihazlarınızın ve hesaplarınızın şifrelerinin güvenli olduğundan emin olun. Açıklamak gerekirse:

- Ne kadar uzun, o kadar iyi. Şifre olarak bir kelime yerine cümle kullanmayı tercih edin.
- Her bir hesabınız için ayrı bir şifre kullanın. Ayrıca şifrelerinizi, bir şifre yöneticisine kaydedin.
- Mümkünse iki adımlı oturum açma yöntemini tercih edin.

02 - Akıllı cihazlarınızın yazılımlarını her zaman doğrudan birinci kaynaktan güncelleyin



- Akıllı cihaz, internet bağlantısı olan cihaz demektir. Örneğin bazı yazıcılar, bebek telsizleri ve kapı zilleri. Aynı zamanda robot süpürgeler de akıllı cihaz kapsamına girer.
- Güncellemeler sayesinde üreticiler, cihazlarınızın her zaman güvende olmasını sağlar. Bu nedenle açılır pencereleri hemen kapatmayın.



03 - Bir virüs tarayıcı kullanın

- Virüs tarayıcılar, cihazlarınızda virüs, zararlı yazılımlar ve kötü amaçlı uygulamalar gibi sorunlar olup olmadığını kontrol eder.



04 - Düzenli olarak yedekleme yapın

- Aksi takdirde hack'lendiğinizde tüm verilerinizi kaybedebilirsiniz. Bu nedenle tedbirli olmak için dosyalarınızın bir kopyasını saklayın.



05 - Önce kontrol edin, sonra tıklayın

- İnternet suçluları e-posta, kısa mesaj veya ödeme talebi yoluyla zararlı bağlantılar gönderiyorlar. Bu yolla sizi kandırarak özel bilgilerinizi paylaşmanızı veya para yollamanızı sağlamaya çalışıyorlar.

Temel güvenlik ile ilgili daha detaylı bilgi almak ister misiniz?
veiliginternetten.nl/5-tips-basisveiligheid adresini ziyaret edin

5 Basistipps für Ihre Online-Sicherheit

Hier ein paar Apps verschicken und dort einige E-Mails. Fotos und Videos über soziale Medien teilen. Videogespräche mit Freunden und Familie. Geld über die Banking-App überweisen. Einloggen beim Finanzamt oder online einen Termin beim Hausarzt vereinbaren. Drahtlos drucken, den Wecker oder die Heizung einstellen und vieles mehr ... Das Internet erleichtert uns das Leben und bereichert es auch.

Von Smartphone über Drucker bis hin zu Instagram und Gmail: Alle Ihre Geräte und Konten müssen optimal gesichert sein. Denn genau wie in der Offline-Welt sind Kriminelle leider auch online aktiv. Wenn Sie diese fünf Maßnahmen beherzigen, schaffen Sie eine gute Ausgangsbasis für Ihre Online-Sicherheit. So machen Sie Cyberkriminellen das Leben schwer.

01 - Verwenden Sie sichere Passwörter für alle Ihre Geräte und Konten. Das heißt:

- Je länger, desto besser. Verwenden Sie eine Passphrase.
- Verwenden Sie für jedes Konto ein anderes Passwort. Bewahren Sie Ihre Passwörter in einem Passwort-Manager auf.
- Verwenden Sie, wenn möglich, die Anmeldung in zwei Schritten.

02 - Führen Sie immer sofort Software-Updates für Ihre intelligenten Geräte durch



- Das sind alle Geräte, die mit dem Internet verbunden sind. Dazu zählen bestimmte Drucker, Babyfone und sogar Türklingeln, aber auch Staubsaugerroboter.
- Mit Updates sorgen die Hersteller dafür, dass die Sicherheit Ihrer Geräte immer auf dem neuesten Stand ist. Klicken Sie diese Pop-ups also nicht einfach weg!



03 - Verwenden Sie einen Virens Scanner

- Ein Virens Scanner überprüft Ihr Gerät auf alle Arten von Problemen wie Viren, Malware und bösartige Apps.



04 - Führen Sie regelmäßige Datensicherungen durch

- Wenn Sie gehackt werden, können Sie alle Daten verlieren. Machen Sie daher sicherheitshalber eine Kopie Ihrer Dateien.



05 - Erst prüfen, dann klicken

- Internet-Kriminelle versenden gefälschte Links per E-Mail, SMS oder Zahlungsaufforderung. Auf diese Weise versuchen sie, an Ihre Daten zu gelangen oder Sie dazu zu bringen, Geld zu überweisen.

Möchten Sie mehr über die grundlegende Sicherheit im Internet erfahren?
Besuchen Sie uns unter [veiliginternetten.nl/5-tips-basisveiligheid](https://www.veiliginternetten.nl/5-tips-basisveiligheid)

5 basistips foar dyn online feiligens

Appje hjir, e-mailsje dêr. Foto's en fideo's diele fia social media. Fideobelje mei freonen en famylje. Jild oermeitsje fia in Tikkie of dyn bank-app. Ynlogge by de Oerheid of húsdokter fia DigiD. Triedleas printsje, it alarm of de ferwaarming yn 'e hûs ynstelle... It ynternet makket it deistich libben foar in soad minsken in stik aardiger en makliker.

It is wichtich om al dyn apparaten en accounts goed te befeiligjen. Fan dyn smartphone oant dyn printer, fan Instagram oant Gmail. Want krekt as yn de offlinewrâld, binne kriminelen spitigernôch ek online aktyf. Mei dizze fiif aksjes soargest derfoar dat dyn online basisfeiligens op oarder is. Sa makkest it foar cyberkriminelen in stik dreger.

01 - Soargje foar feilige wachtwurden foar al dyn apparaten en accounts.

Mei oare wurden:

- Hoe langer, hoe better. Brûk in wachtwurdsin.
- Brûk foar elke account in oar wachtwurd. En bewarje dyn wachtwurden yn in wachtwurdmanager.
- Brûk wêr't dat kin de twastapsproseduere om yn te loggen.

02 - Fier software-updates fan tûke apparaten altyd daliks út



- In tûk apparaat is in apparaat dat mei it ynternet ferbûn is. Lykas guon printers, babyfoans en doarbellens. Mar ek in robotstofsûger.
- Mei updates soargje fabrikanten derfoar dat de befeiliging fan dyn apparaten altyd op oarder is. Klik dy pop-ups dus net fuort!

03 - Brûk in firusscanner



- In firusscanner kontrolearret dyn apparaat op alderhande aaklichheden, lykas firussen, malware, en kwealike apps.

04 - Meitsje geregeld in back-up



- Ast hackt wurdst, kinst alles kwyt wêze. Meitsje dêrom in kopy fan dyn bestannen, foar de wissichheid.

05 - Earst tsjekke, dan klikke



- Ynternetkriminelen ferstjoere fia in e-mail, tekstberjocht of betelfersyk falske linkjes. Sa besykje se dy oer te heljen om gegevens te dielen of jild oer te meitsjen.

Mear witte oer online basisfeiligens? Gean nei: veiliginternetten.nl/5-tips-basisveiligheid