

PROTECT YOUR DEVICES



restena
réseau · sécurité · lu

Our devices have become indispensable. We use them to work, study, check emails, make payments, surf on social networks and more. But they are also cyber criminals' favourite targets. Let's protect them as strongly as we can!



Install an antivirus on all your devices and run regular scans.

There are both free and paid tools. Check reviews or ask your security officer for reliable and secure tools



Run updates of your software and operating system regularly.

Usually your device indicates this automatically, or you can check for available updates yourself



Treat your mobile devices like your wallet.

Don't leave them lying around, don't give them to anybody else and lock them when they are not in use



Be careful with what you download.

Only download apps or programs from trusted sources (e.g. App Store / Play Store) and check user reviews

DID YOU KNOW?

- A reliable virus scanner protects your devices against different types of malware
- Using a pattern password is the least secure way of locking your phone
- Regularly carrying out updates ensures that your device remains secure since these often serve to patch vulnerabilities

HOW CAN YOUR DEVICE GET INFECTED WITH MALWARE?

- Via an external device (e.g. an infected USB stick or external hard drive)
- Through a download (e.g. infected program or app)
- By opening a malicious attachment or clicking on a malicious link

WHAT DOES AN ANTIVIRUS DO?

- Protects you against suspicious websites
- Scans your PC regularly
- Filters fake mails
- Checks the programs you download for malware such as viruses, worms and spyware

CONTACT
csirt@restena.lu

Check connect.geant.org/csm2021 for more tips and useful content!



CYBER HERO @ HOME
CYBER SECURITY MONTH 2021



As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).



GÉANT

PROTÉGEZ VOS APPAREILS



restena
réseau · sécurité · lu

Nos appareils sont devenus indispensables. Nous les utilisons pour travailler, étudier, consulter nos e-mails, effectuer des paiements, surfer sur les réseaux sociaux, etc. Mais ils sont aussi les cibles préférées des cybercriminels. Il est donc important de les protéger le mieux possible !



Installez un antivirus sur tous vos appareils et effectuez des analyses régulières.

Il existe des outils gratuits et payants. Consultez les avis ou demandez à votre responsable de la sécurité de vous indiquer des outils fiables et sûrs.



Exécutez régulièrement les mises à jour de vos logiciels et de votre système d'exploitation.

Généralement, votre appareil vous l'indique automatiquement, ou vous pouvez vérifier vous-même si des mises à jour sont disponibles.



Traitez vos appareils mobiles comme votre portefeuille.

Ne les laissez pas traîner, ne les donnez à personne et verrouillez-les lorsqu'ils ne sont pas utilisés.



Faites attention à ce que vous téléchargez.

Ne téléchargez que des applications ou des programmes provenant de sources fiables (App Store/ Play Store, par exemple) et vérifiez les avis des utilisateurs

LE SAVIEZ-VOUS ?

- Un antivirus fiable protège vos appareils contre différents types de logiciels malveillants
- L'utilisation d'un mot de passe type est le moyen le moins sûr de verrouiller votre téléphone
- L'exécution régulière de mises à jour garantit la sécurité de votre appareil, car elles servent souvent à corriger des vulnérabilités

COMMENT VOTRE APPAREIL PEUT-IL ÊTRE INFECTÉ PAR UN LOGICIEL MALVEILLANT ?

- Via un dispositif externe (par exemple, une clé USB ou un disque dur externe infecté)
- Par un téléchargement (par exemple, un programme ou une application infectés)
- En ouvrant une pièce jointe malveillante ou en cliquant sur un lien malveillant

QUE FAIT UN ANTIVIRUS ?

- Il vous protège contre les sites Web suspects
- Il analyse régulièrement votre PC
- Il filtre les faux e-mails
- Il vérifie que les programmes que vous téléchargez ne contiennent pas de logiciels malveillants tels que des virus, des vers ou des logiciels espions

CONTACT

csirt@restena.lu



As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Consultez connect.geant.org/csm2021 pour plus de conseils et de matériel utile !



SCHÜTZEN SIE IHRE GERÄTE



restena
réseau · sécurité · lu

Unsere Geräte sind unentbehrlich geworden. Wir nutzen sie zum Arbeiten, Studieren, Abrufen von E-Mails, für Zahlungen, zum Surfen in sozialen Netzwerken und vieles mehr. Sie sind aber auch die bevorzugten Ziele von Cyber-Kriminellen. Daher ist es wichtig, sie möglichst wirksam zu schützen!



Installieren Sie ein Antiviren-programm auf all Ihren Geräten und führen Sie regelmäßige Scans durch.

Es gibt sowohl kostenlose als auch kostenpflichtige Tools. Sehen Sie sich Bewertungen an oder fragen Sie Ihren Sicherheitsbeauftragten nach zuverlässigen und sicheren Tools.



Führen Sie regelmäßig Updates Ihrer Software und Ihres Betriebssystems durch.

Normalerweise zeigt Ihr Gerät dies automatisch an, Sie können aber auch selbst nach verfügbaren Updates suchen.



Behandeln Sie Ihre Mobilgeräte wie Ihre Brieftasche.

Lassen Sie sie nicht herumliegen, geben Sie sie nicht weiter und sperren Sie sie, wenn sie nicht benutzt werden.



Seien Sie vorsichtig mit dem, was Sie herunterladen.

Laden Sie nur Anwendungen oder Programme aus vertrauenswürdigen Quellen herunter (z. B. App Store / Play Store) und überprüfen Sie die Nutzerbewertungen

WUSSTEN SIE DAS?

- Ein zuverlässiger Virensch scanner schützt Ihre Geräte vor verschiedenen Arten von Malware
- Die Verwendung eines Musterkennworts ist die unsicherste Art, Ihr Telefon zu sperren
- Regelmäßige Updates sorgen dafür, dass Ihr Gerät sicher bleibt, da diese oft dazu dienen, Sicherheitslücken zu schließen

WIE KANN IHR GERÄT MIT MALWARE INFIZIERT WERDEN?

- Über ein externes Gerät (z. B. einen infizierten USB-Stick oder eine externe Festplatte)
- Durch einen Download (z. B. ein infiziertes Programm oder eine App)
- Durch Öffnen eines bösartigen Anhangs oder Klicken auf einen bösartigen Link

WAS TUT EIN ANTIVIRENPROGRAMM ?

- Es schützt Sie vor verdächtigen Websites
- Es scannt Ihren PC regelmäßig
- Es filtert gefälschte E-Mails
- Es überprüft die Programme, die Sie herunterladen, auf Malware wie Viren, Würmer und Spyware

KONTAKT

csirt@restena.lu

Weitere Tipps und nützliches Material finden Sie auf connect.geant.org/csm2021/!



As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).



SCHÜTZT ÄRE APPARATER



restena
réseau · sécurité · lu

Eis Apparater sinn onverzichtbarginn. Mir benotzen se fir ze schaffen, ze léieren, E-Mailen ze verschécken, Bezuelungen ze maachen, Surfen op sozialen Netzwierker a méi. Leider sinn se awer d'Ziel vun den Cyber-Kriminelle ginn. Dofir ass et wichteg se sou staark wéi méiglech ze schützen.



Installéiert en Antivirus op allen Apparater a maacht regelméisseg Scannen.

Et gëtt béides, gratis a bezuelte Programmer. Préift Bewäertungen oder frot är IT Ekippen fir en zuverlässigen a sécheren Tool.



Maacht regelméisseg Updaten vun ärer Software an Betriebssystem.

Normalerweis weist ären Apparat dëst automatesch un, oder Dir kënnt selwer no neien Updaten kucken.



Behandelt ären Apparat wéi Äre Portmonnie.

Loosst en net ronderëm léien, gitt kengem en deen Dir net kennt, a leet en ewech wann et net am Gebrauch ass.



Sidd virsiichteg mat deem wat Dir erofluet.

Luet nëmmen Apps oder Programmer aus secheren Quellen erof (z.B. App Store / Play Store) a kuckt och d'Benutzer Bewäertungen

WOUSST DIR DAT?

- En zuverlässigen Virusscanner schützt Är Apparater géint verschidden Aarte vu Malware
- E Passwuert aus engem Muster ass dee mannst séchere Wee fir een Telefon ze spären
- Regelméisseg Updaten garantéieren datt den Apparat méi sécher bleift well dës dacks hëlleflechen Schwachstellen ze flécken

WÉI KANN ÄREN APPARAT MAT MALWARE INFIZIERT GINN?

- Iwwer en externen Apparat (z.B. en infizierten USB Stick oder en externen Festplack)
- Duerch en Download (z.B. infizierte Programm oder App)
- Andeems Dir eng béiswëlleg Annex opmaacht oder op e béiswëllege Link klickt

WAT MËSCHT EN ANTIVIRUS?

- Schützt Iech géint verdächtig Websäiten
- Scannt Äre PC regelméisseg
- Filtert gefälscht E-Mailen
- Kontrolléiert d'Programmer déi Dir erofluet op Malware wéi z.B. Virus, Wurm a Spyware.

KONTAKT

csirt@restena.lu

Kuckt och op connect.geant.org/csm2021 fir méi Tipps an aner nützlech Material!



As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

