

# PROTECT YOUR IDENTITY



restena  
réseau · sécurité · .lu

We regularly share online information about ourselves. Our personal data can fall into the hands of cyber criminals. It's our responsibility to protect our digital identity. Think carefully about what you share online and with whom you share it.



*Secure your online accounts*

**Use strong and different passwords for each of your accounts. If you struggle to remember them, use a password manager**



*Enable two factor authentication (2FA).*

**It's a combination of something you know (a password) with something you have (such as an SMS code or a fingerprint)**



*Be aware of what you share on social media.*

**Don't put any important personal information on your profiles. Double-check before accepting friend requests**



*Stay safe while videoconferencing.*

**Protect your meetings with a password. Don't share invite links with others and be careful with screen and file sharing**

## DID YOU KNOW?

- The traces you leave behind when browsing the internet make up your digital footprint.
- Your digital identity consists of any personal data you share online. It is a personal profile that you should be able to control.
- Your digital identity is more valuable than you might think! Hackers can misuse it to make purchases, to open bank accounts but also to create false profiles.

## WHAT SHAPES YOUR DIGITAL FOOTPRINT AND IDENTITY?

- Your usernames and passwords
- Any personal data you share on social media, such as pictures
- Any online forms you fill out (to register for newsletters, to sign petitions, etc.)
- ... and much more

## ALARM SIGNALS

- Inconsistencies in your bank statement or unfamiliar activity on your credit report
- Invoices for things you didn't purchase
- Social media profiles about you that haven't been created by yourself

## CONTACT

[csirt@restena.lu](mailto:csirt@restena.lu)

**Check [connect.geant.org/csm2021](https://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).

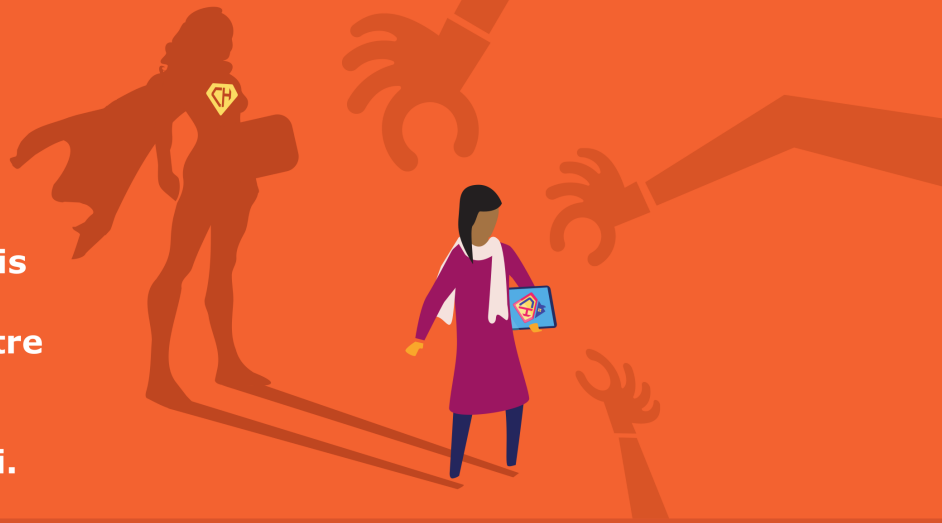


# PROTÉGEZ VOTRE IDENTITÉ



restena  
réseau · sécurité · .lu

À l'ère du numérique, nous partageons en ligne de nombreuses informations nous concernant sans même nous en rendre compte. Mais nos données personnelles peuvent être utilisées à mauvais escient par des cybercriminels. Nous devons donc protéger notre identité numérique et réfléchir soigneusement à ce que nous partageons en ligne et avec qui.



## Sécurisez vos comptes en ligne.

Utilisez des mots de passe forts et différents pour chacun de vos comptes.  
Si vous avez du mal à vous en souvenir, utilisez un gestionnaire de mots de passe.



## Activez l'authentification à deux facteurs (2FA) chaque fois que possible.

C'est comme une deuxième serrure de porte : une combinaison d'un élément que vous connaissez (un mot de passe) et d'un élément que vous avez (comme un code SMS ou une empreinte digitale).



## Faites attention à ce que vous partagez en ligne, notamment sur les réseaux sociaux.

Ne mettez pas d'informations personnelles importantes sur vos profils publics.  
Vérifiez avant d'accepter des demandes d'amis.



## Soyez prudent lors des vidéoconférences.

Protégez vos réunions par un mot de passe. Ne partagez pas les liens d'invitation avec d'autres personnes et soyez prudent avec le partage d'écran et de fichiers.

## LE SAVIEZ-VOUS ?

- Les traces que vous laissez inconsciemment derrière vous lorsque vous naviguez sur l'internet constituent ce que l'on appelle votre empreinte numérique.
- Votre identité numérique est constituée de toutes les données personnelles que vous partagez en ligne. Il s'agit d'une représentation personnelle que vous devriez être en mesure de contrôler.
- Votre identité numérique est plus précieuse que vous ne le pensez ! Les pirates informatiques peuvent l'utiliser à mauvais escient pour effectuer des achats, ouvrir des comptes bancaires, mais aussi pour créer de faux profils.

## QU'EST CE QUI DÉFINIT VOTRE EMPREINTE ET VOTRE IDENTITÉ NUMÉRIQUES ?

- Vos noms d'utilisateur et vos mots de passe.
- Toutes les données personnelles que vous partagez sur les médias sociaux, comme les photos.
- Tous les formulaires en ligne que vous remplissez (pour vous inscrire à des bulletins d'information, pour signer des pétitions, etc.)
- .... et bien plus encore.

## LES SIGNAUX D'ALARME

- Des incohérences dans votre relevé bancaire ou une activité inhabituelle dans votre rapport de carte de crédit.
- Des factures pour des choses que vous n'avez pas achetées.
- Des profils de vous sur les réseaux sociaux que vous n'avez pas créés personnellement.

## CONTACT

[csirt@restena.lu](mailto: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/csm21](https://connect.geant.org/csm21) pour obtenir d'autres conseils et du matériel utile !

# SCHÜTZEN SIE IHRE IDENTITÄT!



restena  
réseau · sécurité · .lu

In diesem digitalen Zeitalter geben wir online viele Informationen über uns preis, ohne es zu erkennen. Unsere persönlichen Daten können jedoch von Cyber-Kriminellen missbraucht werden. Daher müssen wir unsere digitale Identität schützen und gründlich überlegen, was wir online an wen weitergeben.



**Sichern Sie Ihre Online-Accounts.**

Verwenden Sie für jeden Account ein anderes, starkes Passwort. Wenn es Ihnen schwer fällt, sich Passwörter zu merken, verwenden Sie einen Passwortmanager



**Aktivieren Sie nach Möglichkeit die Zwei-Faktor-Authentifizierung (2FA).**

Sie wirkt wie ein zweites Türschloss: eine Kombination aus etwas, das Sie kennen (ein Passwort), und etwas, das Sie haben (wie ein SMS-Code oder ein Fingerabdruck)



**Achten Sie darauf, was Sie online weitergeben, insbesondere auf Social Media.**

Geben Sie in Ihren öffentlichen Profilen keine wichtigen persönlichen Informationen an. Prüfen Sie gründlich, bevor Sie Freundschaftsanfragen annehmen



**Achten Sie auf Ihre Sicherheit bei Videokonferenzen.**

Schützen Sie Ihre Meetings mit einem Passwort. Geben Sie keine Einladungslinks an andere weiter und seien Sie vorsichtig bei der gemeinsamen Nutzung von Bildschirmen und Dateien.

## WUSSTEN SIE DAS?

- Die Spuren, die Sie beim Surfen im Internet unbewusst hinterlassen, sind Ihr so genannter digitaler Fußabdruck.
- Ihre digitale Identität besteht aus allen persönlichen Daten, die Sie online mitteilen. Sie sollten in der Lage sein, diese persönliche Darstellung zu kontrollieren.
- Ihre digitale Identität ist wertvoller als Sie glauben! Hacker können sie missbrauchen, um Einkäufe zu tätigen, Bankkonten zu eröffnen, aber auch um falsche Profile zu erstellen.

## WAS PRÄGT IHREN DIGITALEN FUßABDRUCK UND IHRE IDENTITÄT?

- Ihre Benutzernamen und Passwörter
- Alle persönlichen Daten, die Sie in Social Media weitergeben, beispielsweise Bilder
- Online-Formulare, die Sie ausfüllen (um sich für Newsletter anzumelden, Petitionen zu unterzeichnen usw.)
- ... und vieles mehr.

## ALARMESIGNALE

- Unstimmigkeiten in Ihrem Kontoauszug oder ungewöhnliche Aktivitäten in Ihrer Kreditkartenabrechnung
- Rechnungen für Dinge, die Sie nicht gekauft haben
- Profile von Ihnen auf Social Media, die Sie nicht persönlich angelegt haben

## KONTAKT

[csirt@restena.lu](mailto:csirt@restena.lu)

Weitere Tipps und nützliches Material finden Sie auf [connect.geant.org/csm21/](https://connect.geant.org/csm21/)!



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 ÄR ONLINE IDENTITÉIT!



restena  
réseau · sécurité · .lu

Am digitalen Zäitalter deele mir vill Informatioun iwwer eis online ouni et emol ze mierken. Eis perséinlech Donnéeë kënnen awer leider vu Cyber-Kriminellen mëssbraucht ginn. Dofir ass et wichtig seng digital Identitéit ze schützen a gutt ze iwwerleeën wat mir online deelen a mat wíem.



## Sécher Är Online Konten.

Benutzt staark a verschidde Passwierder fir all Konto. Wann Dir et schwéier fannt ze all ze verhaalen, benutzt e Passwuertmanager



## Aktivéiert zwee Faktor Authentifikatioun(2FA) wa méiglech.

Et ass wéi en zweet Schlass op enger Dier: eng Kombinatioun vun eppes wat Dir wéist (e Passwuert) mat eppes wat Dir hutt (sou wéi en SMS Code oder e Fangerofdrock)



## Sidd Iech bewosst wat Dir online deelt, besonnesch op sozialen Medien.

Deelt keng wichtig perséinlech Informatioun op öffentlechen Profiller. Kontrolléiert léiwer zweemol ier Dir eng nei Frëndes-ufro acceptéiert



## Bleift sécher während Videokonferenzen

Schützt är Reuniounen mat engem Passwuert. Deelt keng Invitatiounslinlen mat aneren a sidd virsichteg mam Écran an Dateien deelen.

## WOUSST DIR DAT?

- D'Spuren déi Dir unbewosst hannerloosst wann Dir um Internet surft sinn ären sougenannten digitalen Foussofdrock.
- Är digital Identitéit besteet aus all de perséinlechen Donnéeën déi Dir online deelt. Et ass eng perséinlech Duerstellung déi Dir sollt kontrolléiere kënnen.
- Är digital Identitéit ass méi wäertvoll wéi Dir denkt! Hacker kënnen se mëssbrauchen fir Akeef ze maachen, Bankkonten opzemaachen awer och fir falsch Profiller ze kreéieren.

## AUS WAT BESTEET DEN DIGITALE FOUSSOFDROCK AN IDENTITÉIT DANN ELO?

- Är Benutzernimm a Passwierder
- All perséinlech Donnéeën déi Dir op sozialen Medien deelt, sou wéi Biller
- All Online Formulieren déi Dir ausfëllt (fir Iech fir Newsletter anzuschreiwén, Petitiounen z'ënnerschreiwén, etc.)
- ... a vill méi.

## ALARM SIGNALER

- Onstëmmegkeeten um Bank Extrait oder unbekannt Aktivitéiten op der Kredittkkaart
- Rechnungen fir Saachen déi Dir net kauft hutt
- Profiller vun Iech op sozialen Medien déi Dir net selwer erstallt hutt

## KONTAKT

[csirt@restena.lu](mailto:csirt@restena.lu)

Kuckt op [connect.geant.org/csm21](https://connect.geant.org/csm21) fir méi Tipps an aner nützlich 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).

