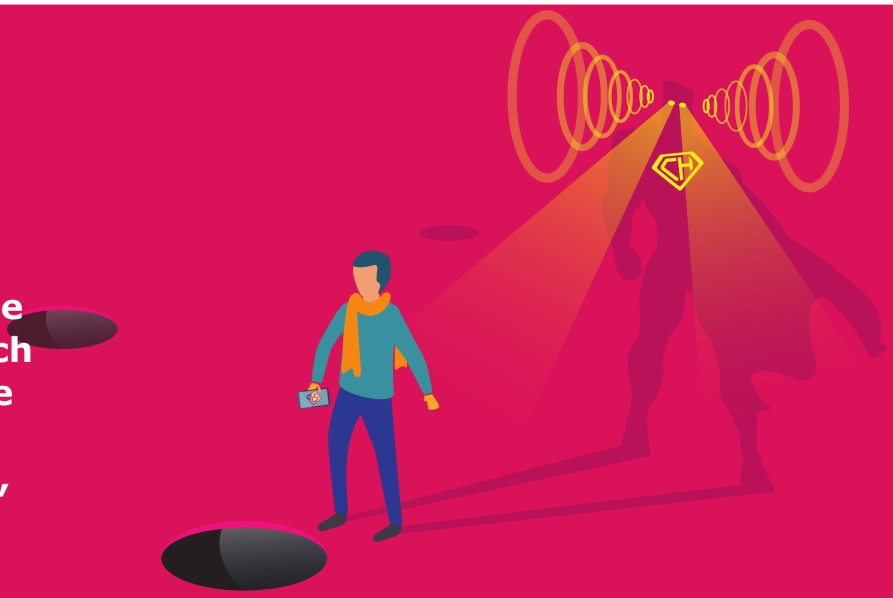
BE AWARE OF CYBERCRIME

restena
réseau · sécurité · .lu

Cybercrime is continuously evolving. Theft, fraud and stalking threaten the online and real worlds alike. Technology cannot guarantee 100% protection against such threats. You are the best line of defence against cybercrime. Protect yourself, stay alert!



Be vigilant when someone asks you to provide personal or confidential information.

The aim of attackers is to get you to act immediately and without thinking

Think before you click.

Do not click on links in an e-mail without thinking. Check the url and look up the website

If something sounds too good to be true, then it probably is.

Don't fall for messages claiming that you have won a smartphone, free tickets or any other prize

Report suspicious messages to your organisation.

By reporting phishing attempts you can help protect others

DID YOU KNOW?

- 84% of cyberattacks rely on social engineering: manipulating someone to reveal personal information or install malicious software
- In recent years ransomware attacks rose 350% and phishing incidents nearly doubled in frequency worldwide

WHAT CAN HAPPEN IF YOU GET HACKED?

- Yours or your company's data can get compromised
- Your device can get infected with ransomware or other types of malware
- Money can be stolen from your bank account

HOW CAN YOU RECOGNISE A PHISHING MAIL?

- The sender uses an email address that does not belong to a legitimate organisation
- The sender asks for something unexpected or out of the ordinary
- The email creates a sense of urgency or arouses your curiosity

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

CONTACT
csirt@restena.lu

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).

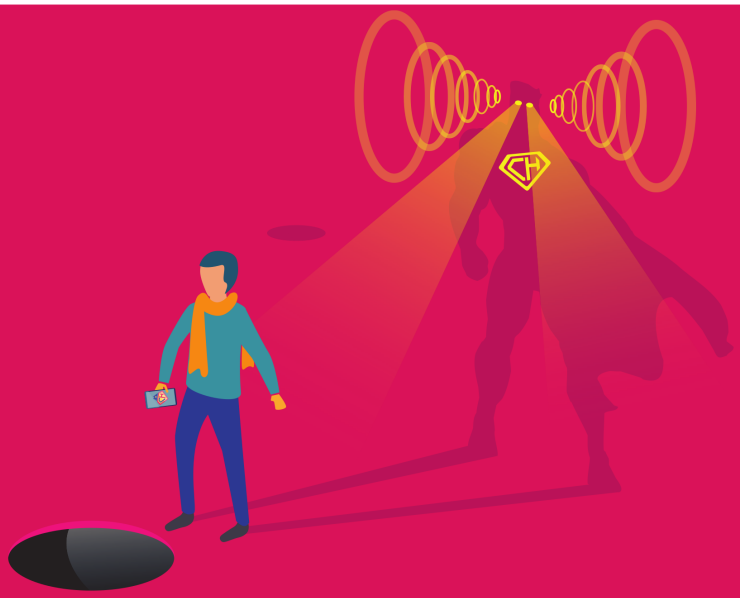
EUROPEAN CYBER SECURITY MONTH

GÉANT

SOYEZ VIGILANT FACE AU CYBERCRIME

restena
réseau · sécurité · .lu

La cybercriminalité est en hausse depuis des années. Le monde en ligne présente des menaces similaires à celles du monde réel, incluant le vol, la fraude et le harcèlement. Vous pouvez vous protéger en restant vigilant. La technologie elle-même ne peut pas vous garantir une protection totale. Vous êtes la meilleure ligne de défense !



Soyez vigilant lorsqu'on vous demande de fournir des informations personnelles ou confidentielles.

L'objectif des cyber-criminels est de vous faire agir immédiatement et sans réfléchir.

Réfléchissez toujours avant de cliquer.

Ne cliquez pas directement sur les liens inclus dans un e-mail, vous pouvez consulter le site internet avant.

Si quelque chose semble trop beau pour être vrai, c'est probablement le cas.

Ne tombez pas dans le piège des messages prétendant que vous avez gagné un smartphone, des billets gratuits ou un autre prix.

Signalez les messages suspects à votre organisation.

En signalant les tentatives de phishing, vous pouvez contribuer à protéger les autres.

LE SAVIEZ-VOUS ?

- 84 % des cyberattaques reposent sur l'ingénierie sociale : il s'agit de manipuler une personne pour qu'elle révèle des informations personnelles ou installe un logiciel malveillant.
- Les attaques de logiciels malveillants dans le monde ont augmenté de 350 % au cours des dernières années.
- Ces dernières années, la fréquence des incidents de phishing a pratiquement doublée.

QUE PEUT-IL VOUS ARRIVER EN CAS DE PIRATAGE ?

- Vos données ou celles de votre entreprise peuvent être compromises.
- Votre appareil peut être infecté par un malware ou d'autres types de logiciels malveillants.
- L'argent de votre compte bancaire peut vous être volé.

COMMENT RECONNAÎTRE UN MAIL DE PHISHING

- L'expéditeur utilise une adresse électronique qui n'appartient pas à une organisation légitime.
- L'expéditeur demande quelque chose d'inattendu ou qui sort de l'ordinaire.
- L'e-mail crée un sentiment d'urgence ou attise votre curiosité.

CONTACT
csirt@restena.lu

Consultez connect.geant.org/csm2021 pour obtenir d'autres conseils et du matériel utile !

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).

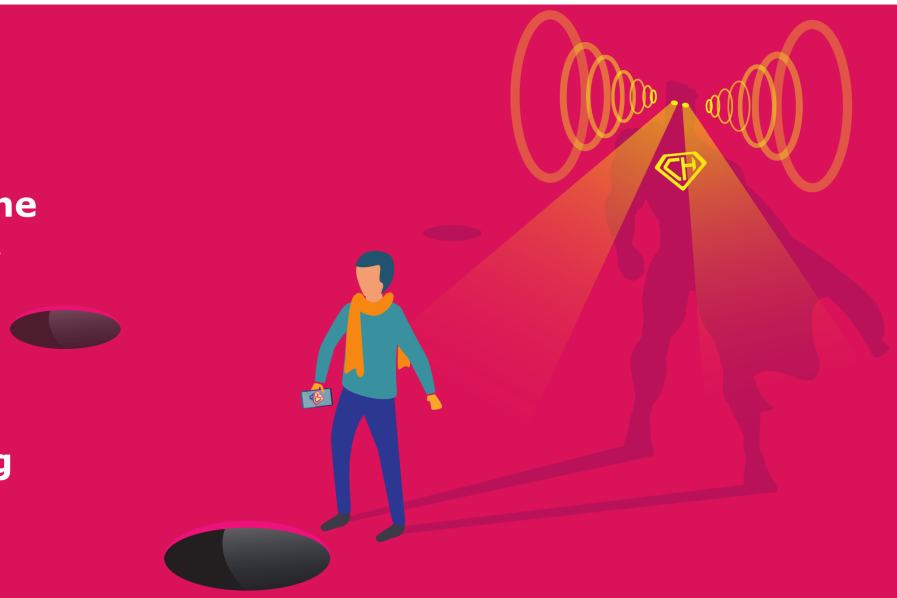
EUROPEAN CYBER SECURITY MONTH

GÉANT

ACHTUNG INTERNETKRIMINALITÄT

restena
réseau · sécurité · .lu

Internetkriminalität ist seit Jahren auf dem Vormarsch. Die Online-Welt birgt ähnliche Gefahren wie die reale Welt, z. B. Diebstahl, Betrug und Stalking. Sie können sich schützen, indem Sie auf der Hut sind. Die Technik selbst kann Sie nicht 100-prozentig schützen. Sie schützen sich selbst am besten!



Seien Sie wachsam, wenn jemand Sie auffordert, persönliche oder vertrauliche Informationen preiszugeben.

Der Angreifer will Sie dazu bringen, sofort und ohne nachzudenken zu handeln.

Erst denken, dann klicken.

Klicken Sie Links in einer E-Mail nicht an, ohne vorher nachzudenken. Suchen Sie die betreffende Website selbst.

Klingt etwas zu schön, um wahr zu sein, ist es in der Regel auch nicht wahr.

Fallen Sie nicht auf Nachrichten herein, in denen behauptet wird, Sie hätten ein Smartphone, kostenlose Tickets oder einen anderen Preis gewonnen.

Melden Sie verdächtige Nachrichten Ihrer Organisation.

Indem Sie Phishing-Versuche melden, können Sie zum Schutz anderer beitragen.

WUSSTEN SIE DAS?

- 84 % der Cyberangriffe beruhen auf Social Engineering: jemanden dazu bringen, persönliche Informationen preiszugeben oder bösartige Software zu installieren
- Ransomware-Angriffe nahmen in den letzten Jahren weltweit um 350 % zu
- In den vergangenen Jahren hat sich die Häufigkeit der Phishing-Versuche nahe zu verdoppelt.

WAS KANN PASSIEREN, WENN SIE GEHACKT WERDEN?

- Ihre Daten oder die Ihres Unternehmens können kompromittiert werden
- Ihr Gerät kann mit Ransomware oder anderen Arten von Malware infiziert werden
- Geld kann von Ihrem Bankkonto gestohlen werden.

WORAN ERKENNEN SIE EINE PHISHING-MAIL?

- Der Absender verwendet eine E-Mail-Adresse, die nicht zu einer rechtmäßigen Organisation gehört
- Der Absender verlangt etwas Unerwartetes oder Außergewöhnliches
- Die E-Mail vermittelt ein Gefühl der Dringlichkeit oder weckt Ihre Neugierde

KONTAKT
csirt@restena.lu

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

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).

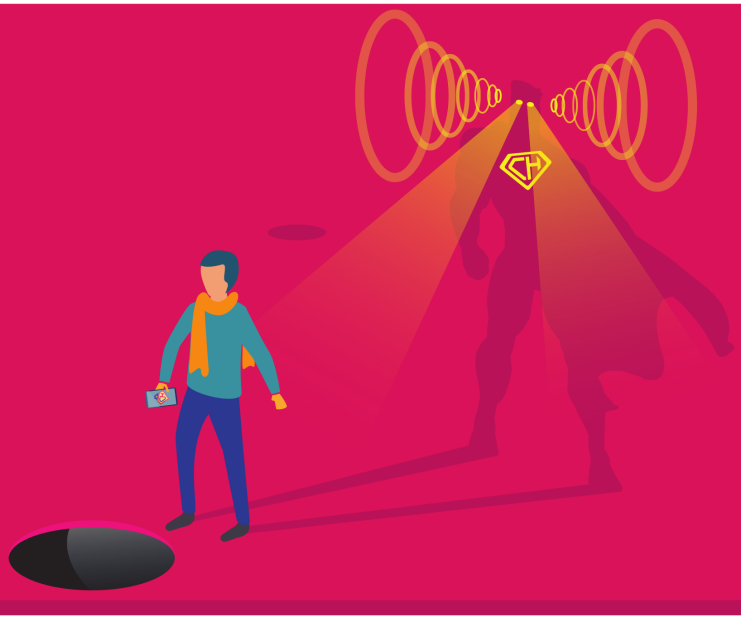
EUROPEAN CYBER SECURITY MONTH

GÉANT

PASS OP CYBER-KRIMINALITÉIT OB

restena
réseau · sécurité · .lu

Cyber-Kriminalitéit geet zënter de leschte Joren erop. D'Online Welt presentéiert ähnlech Gefore fir déi richteg Welt, wie zu Beispill Déifstall, Bedruch a Stalking. Dir kënnt Iech selwer schützen andeems Dir oppasst. Leider kann d'Technologie Iech net zu 100% schützen. Dir selwer bleift dohier nach déi bescht Verdeedegung!



Sidd virsiichteg wann een Iech perséinlech oder vertraulech Informatioun freet.

D'Zil vun den Ugräifer ass Iech ze lackelen fir direkt an ouni ze denken ze handelen.

Denkt ier Dir klickt.

Klickt net op Linken an enger E-Mail ouni ze denken. Kuckt op der Websäit selwer no.

Wann eppes ze gutt kléngt fir wouer ze sinn, dann ass et wahrscheinlech.

Faalt net op Messagen eran déi behaapten datt Dir e Smartphone, Gratis Ticketen oder en anere Präis gewonnen hutt.

Mellt verdächteg Messagen bei ärem Service Informatique.

Andeems Dir Phishing Versich mellt kënnt Dir hëllefen anerer ze schützen.

WOUSST DIR DAT ?

- 84% vun de Cyberattacken vertrauen op Social Engineering Techniken: Et manipuléiert een fir perséinlech Informatioune gewuer ze ginn oder fir béisaarteg Software z'installéieren
- Ransomware Attacken sinn weltwäit em 350% an de leschte Joren
- An de leschte Joren hu Phishing -Tëschefäll hier Frequenz bal verduebelt.

WAT KANN GESCHÉIEN WANN DIR GEHACKT GËTT ?

- Är oder Firma Daten kënnen kompromettéiert oder geklaut ginn
- Ären Apparat kann infizéiert gi mat Ransomware oder aner Aarte vu Malware
- Sue kënne vun Ärem Bankkonto geklaut ginn.

WÉI ERKENNT DIR ENG PHISHING MAIL?

- De Sender benotzt eng E-Mail Adress déi net zu enger legitimer Organisatioun gehéiert
- De Sender freet eppes Onerwaartes oder Aussergewéinleches
- D'E-Mail vermëttelt e Gefill vun Dréngleechkeet oder mécht een gären virwëtzeg méi gewuer ze ginn

Kuckt op connect.geant.org/csm2021 fir méi Tipps an anert nëtzlech Material !

KONTAKT
csirt@restena.lu

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).

EUROPEAN CYBER SECURITY MONTH

GÉANT