Cybermois 2024

Sommaire

Semaine 1

Mardi 1 octobre :

Jour 1 - Introduction
[English version in the thread]
Bonjour @*tous*,

Octobre, le passage à l'heure d'hiver, l'inktober, mais le Cybermois également 🎉

C'est un événement national annuel organisé par différents organismes Français liés à la cybersécurité (cybermalveillance.gouv.fr et l'ANSSI). Il consiste à communiquer sur la prévention et la sensibilisation au risque cyber durant tout le mois d'octobre pour le plus grand monde.

Nous communiquerons donc tous les matins de ce mois-ci de manière très courte sur différents sujets. Soit par quelques lignes, une question, des sondages, ou une petite vidéo de moins de 2 minutes.

Voici donc la vidéo d'aujourd'hui :
https://youtu.be/nTs1kv4N6nI

N'hésitez pas à poser des questions dans le fil de discussion sur des sujets que vous souhaiteriez que l'on aborde.

Le service IT

Day 1 - Introduction
[EN]

Hello everyone,

October, the switch to winter time, inktober, but also Cybermonth 🎉

It is an annual national event organized by different French organizations related to cybersecurity (cybermalveillance.gouv.fr and the ANSSI). It consists of communicating on prevention and awareness of cyber risk throughout the month of October for the greatest number of people.

We will therefore communicate every morning this month in a very short way on different subjects. Either by a few lines, a question, surveys, or a short video of less than 2 minutes.

Here is today's video (You can use the subtitle translator) :

https://youtu.be/nTs1kv4N6nI

Don’t hesitate to ask questions in the discussion thread on subjects that you would like us to address.

IT Team

Mercredi 2 octobre :

Jour 2 - Sauvegarde
@tous [English version in the thread]

Protégez vos données sensibles en toute simplicité !
(papiers d’identité, mots de passe, fiches de paie, photos, etc.)

Avez-vous déjà pensé à ce qui pourrait arriver en cas de panne, de perte de votre matériel, ou même de cyberattaque ? Vos fichiers précieux pourraient disparaître en un instant. 😟

Mais pas de panique ! Il existe des solutions simples pour éviter cela. Pour garantir la sécurité de vos données, pensez à les sauvegarder régulièrement, que ce soit sur un **disque dur externe** ou un **service cloud**.

Voici quelques outils qui pourraient vous aider à mieux protéger vos données :

- **FreeFileSync** pour des sauvegardes sur disque dur.
- **Digiposte**, **kDrive**, **Google Drive**, **OneDrive**, **Amazon Drive** pour des solutions cloud.

Alors, avez-vous déjà mis en place une solution de sauvegarde pour vos données ?
Non ? Alors faites-le avant qu’il ne soit trop tard 😉

—------

Pour plus d’informations / For more informations :

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/sauvegarde-des-donnees-numeriques
- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes
- https://www.cybermalveillance.gouv.fr/medias/2019/11/Fiche-pratique_sauvegardes.pdf

—-------

Effectuez-vous des sauvegardes ?
1- Oui, de manière automatique / Yes, automatically
2- Oui, manuellement tous les mois / Yes, manually every month
3- Une fois par an grand max / One per year
4- Non, pas du tout. Il faut que je le fasse ^^ / Nope at all ^^` I'll do it

Day 2 - Backup
[EN]

Protect your sensitive data with ease!
(ID papers, passwords, payslips, photos, etc.)

Have you ever thought about what could happen in case of a hardware failure, loss of your equipment, or even a cyberattack? Your valuable files could be gone in an instant. 😟

But don't worry! There are simple solutions to avoid this. To ensure the security of your data, make sure to back them up regularly, either on an **external hard drive** or a **cloud service**.

Here are a few tools that can help you better protect your data:
- **FreeFileSync** for backups on an external hard drive.
- **Digiposte**, **kDrive**, **Google Drive**, **OneDrive**, **Amazon Drive** for cloud solutions.

So, have you already set up a backup solution for your data?
No? Then do it before it's too late 😉

Améliorations :
- Proton drive
- Héberger ses données chez soi de manière indépendante (NAS Synology par exemple)

Jeudi 3 octobre :

Jour 3 - Mise à jour
@tous [English version in the thread]

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée.
Les mises à jour ne sont pas là pour ralentir votre poste, mais pour avant tout pour le sécuriser, et également pour apporter de nouvelles fonctionnalités.

Pour résumer :

- Téléchargez les mises à jour uniquement depuis les sites officiels
- Planifiez les mises à jour lors de périodes d'inactivité pour éviter de vous ralentir dans votre travail
- Activez l'option de téléchargement et d'installation automatique des mises à jour
- Attention aux logiciels piratés ! 👀

Pour l'occasion, je vous propose 2 très courtes vidéo sur le sujet :
https://youtu.be/uq44uIcoNOQ
https://youtu.be/UX7Q_V3a_Eg

Pour en savoir plus / For more informations :

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour
- https://www.cybermalveillance.gouv.fr/medias/2020/04/fiche_mises_a_jour.pdf

Day 3 - Update
[EN]

The digital devices and software we use every day are exposed to security vulnerabilities. These vulnerabilities can be used by cybercriminals to take control of a computer, mobile device or even a connected watch.
Updates are not there to slow down your computer, but first and foremost to make it more secure, and also to bring new functionalities.

To sum up :

- Download updates only from official websites
- Schedule updates during periods of inactivity to avoid slowing down your work.
- Enable automatic download and installation of updates
- Watch out for pirated software ! 👀

To mark the occasion, here are 2 very short videos on the subject :

- https://youtu.be/uq44uIcoNOQ
- https://youtu.be/UX7Q_V3a_Eg

Vendredi 4 octobre :

Jour 4 - Verrouillage écran
@tous [English version in the thread]

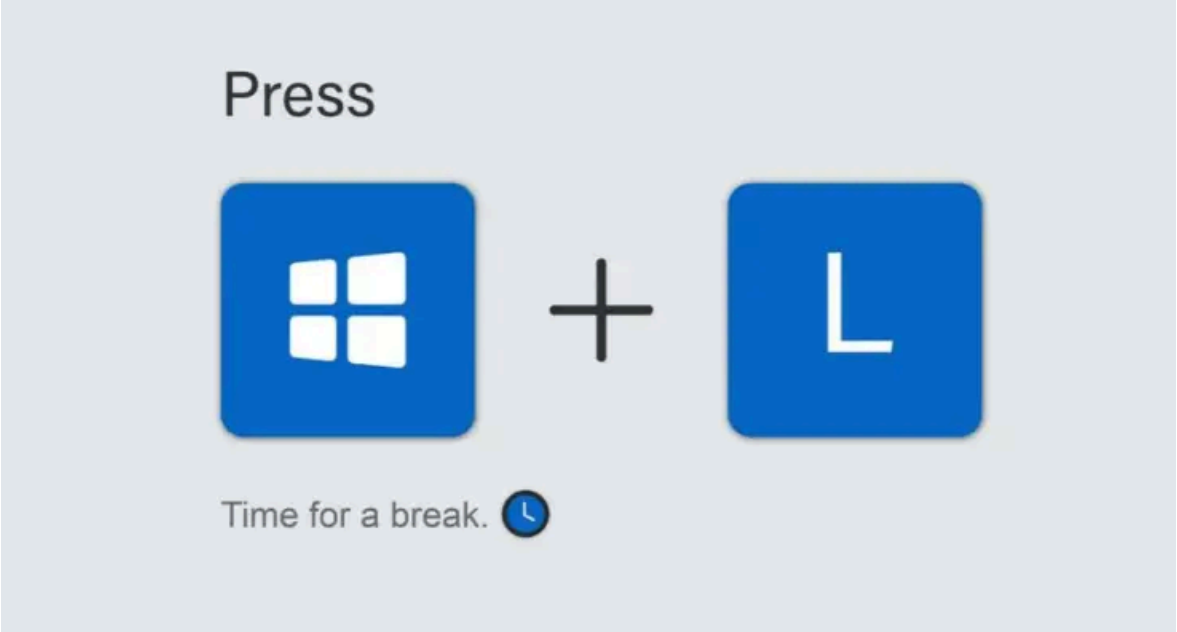
Aujourd'hui va être le jour le plus calme et le plus simple.
Cela prend littéralement moins de 2 clics, enfin plutôt 2 touches de clavier.
À savoir les touches (**Windows + L**)

Si vous appuyez simultanément dessus, cela permet de verrouiller son écran rapidement lorsqu'on part en pause.
Évitant ainsi de potentiels accès frauduleux à votre poste laissé sans surveillance si on est dans le train, ou dans des endroits publics.
D'autant plus si vous avez des fichiers sensibles, ou des droits d'accès élevés.

Alors abusez-en partout, et également au studio ;)

Autre point si vous ne savez pas quoi faire du week-end, vous pouvez cultiver vos compétences numériques sur la plateforme en ligne Pix qui est maintenant obligatoire pour l'obtention du bac.

Le service IT



Day 4 - Lock your screen
[EN]

Today's going to be the easiest day.
It literally takes less than 2 clicks, or rather 2 keyboard strokes.
Namely, the keys (Windows + L)

If you press it simultaneously, it locks your screen quickly when you're on a break.
This prevents unauthorized access to your unattended computer when you're on the train, or in public places.
Especially if you have sensitive files or high access rights.

So use it everywhere, and in the studio too ;)

And if you don't know what to do on the weekend, you can cultivate your digital skills on the Pix online platform, which is now compulsory for French baccalaureate.

IT Team

Semaine 2 - Mot de passe

Lundi 7 octobre :

Jour 5 - Un bon mot de passe

Bonjour @*tous [English version in the thread]*
Cette semaine on attaque un gros morceau.
On va se concentrer spécifiquement sur les mots de passe. Vous inquiétez pas, ça va bien se passer.

Un bon mot de passe, selon la CNIL (Commission nationale de l'informatique et des libertés) c'est au moins 12 caractères comprenant 4 types de caractères différents (Reference) :

- Minuscules
- Majuscules
- Chiffres
- Caractères spéciaux.

Pour la faire courte, votre mot de passe doit avoir une complexité forte. Cette dernière appelée "entropie" peut-être calculée par différents outils que nous verrons au cours de la semaine.
Pour information, la CNIL recommande d'avoir une entropie de 80 minimum.

Ok, mais vu que le mot de passe est long, comment faire pour le retenir ?
Vous pouvez utiliser des phrases de passes qui vous permettront de vous en souvenir.
Par exemple :
Votre tortue s'appelle Georgette et vous habitez en Charente-Maritime.

Ce qui donnerait :
VOILÀ_LA_TORTUE_DU17

Vous pouvez également utiliser des phrases de passe avec la méthode diceware ou par l'outil de la CNIL.

====En commentaire thread====

Pour aller plus loin :

- https://cyber.gouv.fr/cybermois-2021-les-mots-de-passe
- https://www.cnil.fr/fr/verifier-sa-politique-de-mots-de-passe
- https://nothing2hide.org/fr/verifier-la-robustesse-de-votre-mot-de-passe/

Mon avis :
La CNIL recommande d'avoir une entropie de 80 minimum, mais personnellement je vous conseillerais de toujours avoir un coup d'avance dessus et de se baser sur une entropie de 100 minimum.

Bien sûr la complexité de votre mot de passe cela dépend du contexte d'utilisation que vous en faîtes (Mail principal, comptes bancaire, agence de voyage, musées, etc..) et de ses protections qui lui sont associés (Filtrage par adresse IP de connexion ou équipements, blocage lors de trop de tentatives échoués, authentification multi-facteur).

Day 5 - A good password
[EN]

This week we are tackling a big chunk.

We will focus specifically on passwords.
Don't worry, it will go well.

A good password, according to the CNIL (National Commission for Information Technology and Liberties) is at least 12 characters including 4 different types of characters (Reference) :

- Lowercase
- Uppercase
- Numbers
- Special characters.

To make it short, your password must have a high complexity. The latter called "entropy" can be calculated by different tools that we will see during the week.
For information, the CNIL recommends having an entropy of at least 80.

Ok, but since the password is long, how can you remember it?
You can use passphrases that will help you remember it.
For example :
Your turtle is called Georgette and you live in New-York City.

Which would give :
HEERE_IS_MY_TURTLE_OF1001

You can also use passphrases with the diceware method or by the CNIL tool.

Mardi 8 octobre :

Jour 6 - Double authentification
@tous [English version in the thread]

Un bon mot de passe c'est bien, mais défois ça ne suffit pas.
https://www.dailymotion.com/video/x8nt02t

C'est pourquoi il est recommandé d'activer la double authentification, offrant une couche de protection supplémentaire. Même si votre mot de passe est volé, l'assaillant devra entrer un code temporaire pour accéder à votre compte.

Cette double authentification peut se faire de différentes manières :

- Via un autre canal : SMS, Appel téléphonique, Email, Application d'authentification
- Physique: Clé USB
- Biométrique: Empreinte digitale, scan rétinien

Le plus simple étant d'utiliser une application d'authentification sur téléphone. Car elle est facile d'accès, utilisable même en mode hors-ligne, et peut être synchronisée sur différents appareils.

Différentes solutions existent : Google authenticator, Microsoft Authenticator, Aegis, etc..

N'hésitez pas à l'activer sur tous vos comptes lorsque c'est possible.

Le service IT

====Commentaire====

N'oubliez pas d'enregistrer votre code de récupération lors de l'activation de la double authentification en cas d'inaccessibilité à votre application d'authentification. Ainsi que de synchroniser vos codes d'authentification via votre compte mail.

Day 6 - Authentication multiple
[EN]

A good password is good, but sometimes it's not enough.
https://www.dailymotion.com/video/x8nt02t

That's why it is recommended to activate two-factor authentication, which offers an additional layer of protection. Even if your password is stolen, the attacker will have to enter a temporary code to access your account.

This two-factor authentication can be done in different ways :

- Via another channel : SMS, Phone call, Email, Authentication application
- Physical: USB key
- Biometric: Fingerprint, retinal scan

The simplest is to use an authentication application on your phone. Because it is easy to access, usable even in offline mode, and can be synchronized on different devices.

Different solutions exist: Google authenticator, Microsoft Authenticator, Aegis, etc.

Do not hesitate to activate it on all your accounts when possible.

IT department

====Comment====

Don't forget to save your recovery code when activating two-factor authentication in case your authentication application is inaccessible. As well as synchronizing your authentication codes via your email account.

Mercredi 9 octobre :

Jour 7 - Un mot de passe unique et différent pour chaque usage
@tous [English version in the thread]

Je vous vois déjà lever les yeux en l'air juste en lisant le titre du jour.
"Aller, maintenant ils veulent qu'on mette des mots de passes complexes partout…"

Mais pourquoi c'est important ?
Si un site où vous vous êtes inscrit venait à être hacker, il y a des chances que votre mot de passe que vous avez utilisé là bas puisse être récupéré par les hackeurs.
Et donc, que ces derniers puissent le réutiliser sur d'autres plateformes où vous vous êtes inscrits.

Mais pas de panique, demain on vous expliquera comment faire pour organiser tout ça ;)

PS: À moins que vous ne vous appeliez Elon Musk, ne suivez pas cette fausse bonne idée.

Le service IT

Day 7 - Unique and different password for each usage
[EN]

I can already see you rolling your eyes just reading today's headline.
"Come on, now they want us to put complex passwords everywhere..."

But why does it matter?
If one of your account passwords is compromised, whether by a data leak, a brute force attack, phishing (more on that later), etc., it means that all your other accounts are compromised.
This means that all your other account passwords are also compromised.

But don't panic, tomorrow we'll explain how to organize all this ;)

PS: Unless your name is Elon Musk, don't follow this false good idea.

IT Team


FAUSSE BONNE IDÉE N°3
“La barbe... Si je change de mot de passe je vais devoir changer le nom de mon fils pour m’en souvenir !”
CONSEIL :
UTILISEZ DES MOTS DE PASSE COMPLEXES ET DIFFÉRENTS PARTOUT

Jeudi 10 octobre :

Jour 8 - Gestionnaire mot de passe
@tous [English version in the thread]

Pour vous éviter de vous faire des nœuds au cerveau en retenant tous vos mots de passe.
Ou les noter à droite, à gauche sur des posts-it à côté de votre écran 👀
Il est plus sécurisé et facile d'utilisation de les enregistrer dans un gestionnaire de mots de passe qui centralise vos différents accès.

Pour ce faire, il existe différentes solutions :

- Via navigateur web : Google Chrome, Mozilla Firefox, etc..
- Via un site web dédié : Google (Gratuit), Bitwarden, Proton pass (tous 2 gratuits jusqu'à un certain niveau)
- En local sur votre poste (pour utilisateur avancé) : Keepass (gratuit)

De notre côté, nous travaillons actuellement sur la mise en place d'une plateforme de gestionnaire de mots de passe en interne. Cela vous permettra d'appréhender le sujet.

Le service IT

Day 8 - Vault password
[EN]

To avoid the torture of remembering all of your passwords.
Or write them down here and there on post-it notes next to your screen 👀
It's easier and more secure to save them in a password manager that centralizes your various accesses.

There are several solutions for this:

- Via a web browser: Google Chrome, Mozilla Firefox, etc.
- Via a dedicated website: Google (Free), Bitwarden, Proton pass (both are free up to a certain level)
- Locally on your workstation (for advanced users): Keepass (free)

For our part, we're currently working on setting up an in-house password management platform. This will enable you to get to grips with the subject.

IT Team

Vendredi 11 octobre :

Jour 9 - Vérification fuite de données
@tous [English version in the thread]

Pour être proactif, et vérifier si votre adresse mail, votre numéro de téléphone ou un de vos anciens mot de passe ont fuité dans des brèches de données publiques, vous pouvez utiliser les sites suivants :

- https://haveibeenpwned.com/
- https://haveibeenpwned.com/Passwords

Cette plateforme vous propose également une possibilité de vous notifier si votre adresse mail se trouve dans une nouvelle brèche, vous permettant d'être plus vigilant face à l'augmentation des tentatives de phishing (faux e-mails).

Pour information, la grande majorité des logiciels de gestionnaire de mots de passe que nous avons évoqué hier intègrent cette fonctionnalité de vérification pour savoir si vos mots de passe ont été compromis.

Pour voir si vous avez bien compris les différentes recommandations de cette semaine, je vous invite à lire cette BD à choix multiple sur le sujet :
https://cyber.gouv.fr/sites/default/files/2022-09/anssi-cybermois_2021-bd_hugo%5B1%5D.pdf

Day 9 - Check data breach
[EN]

To be proactive, and check out if your email address, phone number or any of your old passwords have leaked into public data breaches, you can use these sites:

- https://haveibeenpwned.com/
- https://haveibeenpwned.com/Passwords

It also offers the option of notifying you if your e-mail address is in a new breach. This allows you to be more vigilant in the event of a rise in bogus e-mails.

For your information, the vast majority of the password manager software we mentioned yesterday have this verification feature to find out if your password has been compromised.

To see if you've understood this week's recommendations, take a look at this multiple-choice comic strip on the subject:
https://cyber.gouv.fr/sites/default/files/2022-09/anssi-cybermois_2021-bd_hugo%5B1%5D.pdf

Mon avis :
La CNIL, et L'ANSSI ne recommande plus de changer de mot de passe :
https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite

Cela peut être en effet une mesure qui peut être appliquée, seulement si le compte est protégé par d'autres moyens supplémentaires (Double authentification, limitation connexion par tentatives/IP/Appareils).

Semaine 3

Lundi 14 octobre :

Jour 10 - Périphériques amovibles
@tous [English version in the thread]

Oh ! Je viens de trouver une clé usb dans la rue, je vais la brancher sur mon PC ce soir pour voir ce qu'il y a à l'intérieur.
! **Attention** !

Cette clé usb peut contenir un programme malveillant pouvant s'exécuter automatiquement sur votre poste. Ce dernier pourrait ainsi installer un autre programme malveillant, chiffrer vos données ou récupérer vos données personnelles.
Le branchement de cette clé usb peut également créer un court-circuit sur votre poste le rendant inutilisable.

Quelques bonnes pratiques sont de rigueur lorsque vous utilisez des appareils de stockage externe, comme des clés USB ou des disques durs externes :

- N'utilisez jamais un service ou un équipement inconnu ou abandonné.
- Attribuez un usage spécifique à chaque clé USB pour réduire les effets d'une éventuelle contamination.

En cas de doute, je n'y touche pas ou je transmet l'équipement au service informatique ou à l'accueil.

Toujours pas convaincue ?
Voici une vidéo à savourer :
https://youtu.be/xCLboWLVia0

Day 10 - External devices
[EN]

Oh, I just found a USB flash drive in the street, I'm going to plug it into my PC tonight and see what's inside.
! **Warning** !

This USB flash drive may contain a malicious program that can run automatically on your computer. This could install another malicious program, encrypt your data or steal your personal data.
Plugin a USB flash drive can also create an electrical short-circuit on your computer, breaking it.

When using external storage devices, such as USB flash drive or external hard drives,

there are a few best practices to follow:

- Never use unknown or abandoned equipment or services.
- Assign a specific use to each USB key to reduce the effects of possible contamination.

If in doubt, leave it alone or pass it on to the IT department or reception.

Still not convinced?
Enjoy this video :
https://youtu.be/xCLboWLVia0

Mardi 15 octobre :

Jour 11 - Antivirus
@tous [English version in the thread]

Un anti-virus s'appuie sur des "bases de signatures" qui permettent d'identifier des logiciels malveillants installés ou exécutés sur votre ordinateur, mais également dans la mémoire, le(s) disque(s) dur(s), le contenu de vos messages (email), le contenu des pages web, les supports amovibles (clé usb, dvd, ..).
Certains d'entre eux permettent également d'analyser des comportements anormaux qui pourraient être liés à des virus.

Mon avis :
L'antivirus de Windows (Windows Defender) qui est installé par défaut est très performant dorénavant et peut se suffire à lui-même.

Mais vous pouvez également utiliser un autre anti-virus qui prendra la place de celui par défaut.
Quelques recommandations cependant :

- Prenez en un payant (quand c'est gratuit, c'est vous le produit. Vos données personnelles peuvent être revendues, et cet outil à accès à toutes vos données sur votre poste)
- Privilégier des solutions Française, Européenne, ou Américaine pour éviter le vol de données également

==========

Pour plus d'informations / For more informations :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus

Day 11 - Antivirus
[EN]

An antivirus is based on “signature databases” to identify malicious software installed or running on your computer, but also in your memory, hard disk(s), the content of your messages (email), the content of web pages, removable media (usb key, dvd, ...).
Some of them can also analyze abnormal behavior that could be linked to viruses.

My opinion :
The Windows antivirus (Windows Defender) installed by default is now very powerful and can stand alone.

But you can also use another antivirus program to replace the default one.
A few recommendations, however :

- Get a paid one (when it's free, you're the product. Your personal data can be sold, and this tool has access to all your data on your workstation).
- Choose French, European or American solutions to avoid data theft too.

Mon avis :
L’antivirus de Microsoft qui est derrière celui de Windows connaît très bien sa solution vu que c’est eux-même qui sont les “constructeurs” du système Windows.

Mercredi 16 octobre :

Jour 12 - Envoie d'informations de manière sécurisé
@tous [English version in the thread]

Sûrement vous est-il déjà arrivé d'envoyer des justificatifs d'identité pour un nouvel emploi, louer un appartement ou d'autres démarches personnelles.

Vous les envoyez en pièce jointe par mail ? D'accord, mais si un attaquant accède à votre boite mail ou à celle de votre destinataire, il aura accès à tous les documents que vous aurez envoyés.
Donc comment contrôler l'envoie de ses informations de façon sécurisée et confidentielle ? Et empêcher la potentielle utilisation illégitime de ses données pour usurper votre identité ?

La bonne pratique est d'envoyer un lien qui redirigera vers une plateforme extérieure où vos documents seront accessibles. Cet espace de stockage devra avoir un mot de passe et une limitation d'accès dans le temps.

Je vous propose ses solutions gratuites possibles :

- Swiss Transfer (Création lien avec durée de validité, limite de téléchargement, protégé par mot de passe, hébergement en Suisse, sans compte nécessaire)
- Digiposte (Création lien de partage temporaire avec mot de passe, hébergé en France 🐓)

Cela évite l'envoie de documents en clair dans vos mails ✅
Mais ne restreint pas son utilisation hors du cadre prévue* 🛑
**Voir commentaires pour autres solutions répondant à ce besoin*

Et vous, quels risques êtes-vous prêt à prendre ?
Allez-vous changer vos habitudes 😶 ?

==========

Plus spécifiquement, d'autres solutions alternatives existent par exemple l'État propose via le biais de France Identité, permet de générer des justificatifs d'identité à usage unique.
Cela permet de prouver son identité sans communiquer le visuel de sa pièce d'identité, tout en limitant son utilisation pour un cadre précis.

D'autre part, pour la création d'un dossier logement, l'état met à disposition la plateforme Dossier facile qui permet de valider votre dossier côté locataire ou propriétaire, et de ne le transmettre qu'à la personne désiré pour une durée déterminée avec un filigrane sur vos documents. Il est possible également d'ajouter des filigranes pour un document spécifique via filigrane facile.
Cependant il peut facilement être enlevé 🛑 je ne vous apprend rien, vous le savez déjà.

Day 12 - Send information securely
[EN]

Have you ever had to send proof of identity for a new job, renting an apartment or other personal reasons?

Do you send them as email attachments? Okay, but if a hacker gains access to your mailbox or that of your recipient, he'll have access to all the documents you've sent.
So how can you control the secure and confidential transmission of your information?
And prevent the potential illegitimate use of your data to impersonate you?

The best practice is to send a link that redirects to an external platform where your documents can be accessed. This storage space should be password-protected and time-limited.

Here are some possible free solutions :

- Swiss Transfer (Link with validity period, download limit, password protection, hosted in Switzerland, no account required)
- Digiposte (temporary sharing link with password, hosted in France 🐓)

This avoids sending unencrypted documents in your emails ✅
But doesn't restrict its use outside its intended scope* 🛑
**See comments for other solutions meeting this need*

And you, what risks are you disposed to take?
Are you going to change your habits 😶 ?

=========

More specifically, other alternative solutions exist, such as the French government's proposal, via France Identité (for French citizens), to generate single-use identity documents.
This enables you to prove your identity without having to provide the visual of your identity document, while limiting its use to a specific context.

In addition, to create a housing file, the French government provides the Dossier facile platform, which enables you to validate your file on the tenant or owner side, and to transmit it only to the person you wish for a given period of time, with a watermark on your documents. It is also possible to add watermarks for a specific document via filigrane facile.
However it can easily be removed 🛑 I'm not teaching you anything you don't already know.

Envoie mdp / fichier :

- Swiss Transfer
- Password pusher

Sinon, vous pouvez toujours transmettre vos documents par support amovibles (clés usb, disque dur) si vous chiffrer le contenu pour éviter le vol de données (Via Bitlocker to Go par exemple)

Jeudi 17 octobre :

Jour 13 - Séparation usage Pro / Perso
@tous [English version in the thread]

Séparer vos usages fait partie des bonnes pratiques à mettre en place.
En effet, si vous synchronisez vos mots de passe, favoris, et historiques de vos comptes pro sur vos comptes personnels ou vice-versa, cela permettrait à un cybercriminel ayant l'accès à un de vos comptes de récupérer des informations personnelles d'un autre de vos usages.
De plus, par soucis de votre vie privée nous vous conseillons de séparer ces usages.

Voici quelques bonnes pratiques sur le sujet :

- Différencier vos comptes (au minimum Personnel / Professionnel / Travail)
- Différencier votre profil de navigateur web, ou mieux votre navigateur web selon vos usages :
    - Google Chrome/Brave pris en compte nativement
    - Firefox via l'extension "Firefox Multi-Account Containers"
    - Safari pris en compte nativement
- Ne pas utiliser des services de stockage personnel à des fins professionnelles

==========

Pour plus d'informations / For more informations :

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso
- https://www.cybermalveillance.gouv.fr/medias/2019/11/Fiche-pratique_usages-pro-perso.pdf

Day 13 - Split Pro / Perso usage
[EN]

Separating your usages is one of the best practices you can implement.
Indeed, if you synchronize your passwords, bookmarks and history from your business accounts to your personal accounts, or vice versa, this would enable a cybercriminal with access to one of your accounts to retrieve personal information from another of your usages.
What's more, out of concern for your privacy, you may also wish to separate your usages.

Here are a few best practices on the subject :

- Differentiate your accounts (at least Personal / Professional / Work)
- Differentiate your web browser profile, or better still your web browser according to your usages :
    - Google Chrome/Brave natively supported
    - Firefox via the extension "Firefox Multi-Account Containers"
    - Safari natively supported
- Do not use personal storage services for professional purposes

Source :
https://www.kaspersky.fr/blog/disable-browser-sync-enterprise/20312/

Vendredi 18 octobre :

Jour 14 - Usurpation d'identité
@tous [English version in the thread]

Qu'est-ce que l'usurpation d'identité ?
C'est le fait d'utiliser des informations personnelles permettant d'identifier une personne sans son accord pour réaliser des actions frauduleuses.
Que ce soit par quelqu'un qui se fait passer pour vous auprès d'une agence immobilière, de la CAF, etc.. pour récupérer de l'argent ou plus d'informations personnelles vous concernant.
Ou inversement, une personne qui entre en contact avec vous en se faisant passer pour un organisme (Impôts,police) en vous demandant des informations, de l'argent, etc..

Nous reviendrons plus en détail sur ces dérivés durant la semaine prochaine qui sera concentrée sur le domaine de l'arnaque en ligne.

Comment réagir et signaler que vous êtes victime d'une usurpation d'identité ?

- Sauvegarder les preuves en votre possession
- Signaler directement l'usurpation d'identité auprès des plateformes sur lesquelles elle a lieu
- Déposer plainte au commissariat / brigade de gendarmerie dont vous dépendez
- Voir suite sur Cybermalveillance.gouv.fr - Partie 3

Comment réagir en amont pour éviter une usurpation d'identité ?

- Ne communiquez jamais d'informations personnelles sensibles à des personnes ou organismes que vous n'avez pas authentifiés avec certitude
- Faites attention à qui vous parlez sur Internet ou par téléphone
- Ne donnez que le minimum d'informations personnelles indispensables (Utiliser un pseudonyme au lieu de votre nom/prénom)

Voici une petite vidéo sur le sujet :
https://youtu.be/LdKABps3LZA

==========

Pour plus d'informations / For more informations :

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/usurpation-identite-que-faire
- https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite
- https://www.economie.gouv.fr/particuliers/protection-usurpation-identite#

Day 14 - ID Fraud
[EN]

What is identity theft?
It's the act of using personal identifying information without a person's consent to carry out fraudulent actions.
Whether it's someone impersonating you at an estate agency, the ACA (Affordable Care Act), etc., to get money or more personal information about you.
Or conversely, a person who contacts you posing as an organization (tax office, police) asking for information, money, etc...

We'll be coming back to these derivatives in more detail next week, when we'll be concentrating on online scams.

How to react and report identity theft ?

- Save the evidence in your possession
- Report identity theft directly to the platforms on which it is taking place
- File a complaint with your local police station
- See next steps on Cybermalveillance.gouv.fr - Part 3

How can I prevent identity theft from happening in the first place ?

- Never communicate sensitive personal information to people or organizations you haven't authenticated with certainty.
- Be careful who you talk to on the Internet or by telephone
- Give only the minimum amount of essential personal information (use a pseudonym instead of your first or last name).

Here is today's video :
https://youtu.be/LdKABps3LZA

Semaine 4 - Arnaque en ligne

Lundi 21 octobre :

Jour 15 - Phishing
@tous [English version in the thread]

Ce terme définit l'utilisation d'un faux message envoyé par mail par un cybercriminel qui usurpe l'identité d'une personne, comme votre enfant qui aurait perdu son téléphone, ou un organisme tiers comme une banque, un site de commerce, la crèche de votre enfant, votre club de sport, ou autre…pour vous soutirer vos mots de passe ou de l'argent via un lien vous redirigeant vers un faux site web de l'organisme, par exemple.

Bien que souvent envoyé par mail, des dérivés du phishing existent également :

- Vishing : Arnaques par appels téléphoniques
- Smishing : Arnaques par SMS
- Quishing : Arnaques par QRCodes placés sur des QRCodes légitimes
- Spear phishing : Phishing avancé vous ciblant spécifiquement avec des informations personnelles récupérées sur vous (date de naissance, collègue de travail, etc..)

Comment réagir ?
Premièrement, identifier la situation :

- Situation d'urgence ?
- Forte émotion ressentie ?
- Fautes d'orthographes ?
- Tentative de gagner votre confiance ?
- Est-ce absurde ?

Si vous avez répondu "**oui**" à l'une ou plusieurs de ces questions, faites très attention ! Votre interlocuteur est sûrement un escroc.

En cas de doute, n'alimentez pas la menace.
Ne répondez pas, ne cliquez pas.
Signalez le message et supprimez-le.

Quelques bonnes pratiques supplémentaires :

- Ne communiquez jamais d'informations sensibles par SMS
- Ne cliquez jamais sur les liens dont vous ne connaissez pas la provenance
- Vérifier l'information directement sur le site officiel de l'organisme

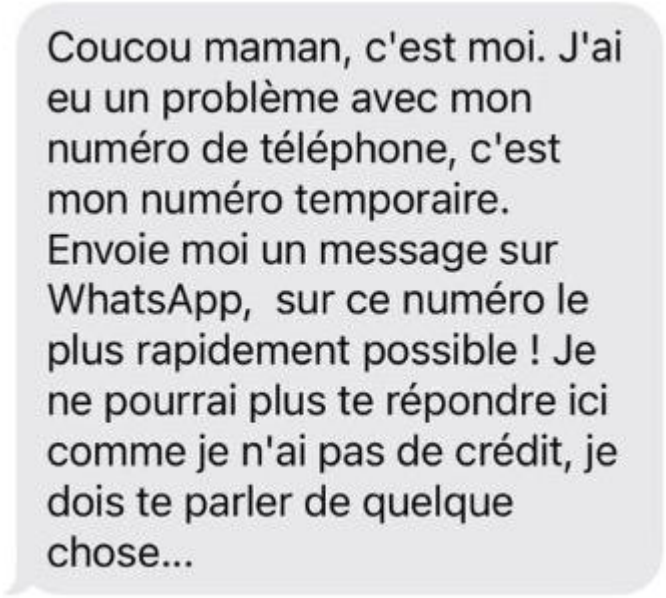
=====

Pour aller plus loin, vous pouvez signaler ces pratiques via ces différents sites :

- Liens frauduleux : Phishing initiative
- Appels/messages frauduleux à transférer par sms au **33 700** (https://www.33700.fr/)
- Démarchage téléphonique / SMS : https://www.bloctel.gouv.fr/
- Spam mail : https://www.signal-spam.fr/
- Pour anglophone - Action Fraud ou par téléphone : 0300 123 2040

Plus globalement :
- Dispositif Thesee : https://www.service-public.fr/particuliers/vosdroits/N31138
- Contenue illicite : Pharos
- Plainte en ligne : Thesee

Petite vidéo bonus sur le sujet :
https://youtu.be/meFcz_DZKdE



Day 15 - Phishing
[EN]

This term defines the use of a fake e-mail message sent by a cybercriminal who impersonates a person, such as your child who has lost his or her phone, or a third-party organization such as a bank, a shopping site, your child's daycare center, your sports club, or other...to trick you into giving up your passwords or money via a link redirecting you to the organization's fake website, for example.

Although often sent by e-mail, phishing derivatives also exist:
- Vishing : phone call scams
- Smishing : SMS scams
- Quishing : Scams using QRCodes placed on legitimate QRCodes
- Spear phishing : Advanced phishing specifically targeting you with personal information (date of birth, work colleague, etc.).

How to react?
First, identify the situation :

- Emergency situation ?
- Emotional sensations ?
- Misspellings ?
- Attempt to gain your trust ?
- Is it absurd ?

If you answered “**yes**” to one or more of these questions, be very careful! Your interlocutor is probably a swindler.

If you have any doubt, don't reply or click.
Report the message and delete it.

A few additional best practices:

- Never communicate sensitive information by SMS
- Never click on links you don't know the source of.
- Check the information directly on the organization's official website.

=====

To find out more, you can report these practices on the following websites:

- EN : Action Fraud or by telephone: 0300 123 2040
- Fraudulent links : Phishing initiative
- Fraudulent calls/messages to be forwarded by SMS to 33 700 (https://www.33700.fr/)
- Phone / SMS prospecting : https://www.bloctel.gouv.fr/
- Spam mail : https://www.signal-spam.fr/

Global use case :

- Thesee system : https://www.service-public.fr/particuliers/vosdroits/N31138
- Illegal content : Pharos
- Online complaint : Thesee

Bonus video for this subject :
https://youtu.be/meFcz_DZKdE

Mardi 22 octobre :

Jour 16 - Rançongiciel
@tous [English version in the thread]

L'arnaque au rançongiciel est une méthode utilisant un logiciel malveillant qui bloque votre ordinateur et rend tous vos contenus informatiques inaccessibles.
Par la suite, le logiciel demande une rançon pour la récupération des données ou sa non diffusion sur internet avec souvent un compte à rebours affiché sur l'écran.
Ce type de logiciel apparaît lorsque vous installez un logiciel piraté, ou que vous ouvrez une pièce-jointe, un fichier ou un lien vérolé.

Comment réagir si vous êtes victime de ce type d'arnaque ?
Ne payez jamais les rançons !
Vous ne serez pas sûr de récupérer vos données, et le logiciel malveillant peut toujours être actif sur votre équipement.

- Débrancher votre équipement du réseau (par filaire, wifi, partage de connexion)
- N'éteignez pas votre équipement : le logiciel pourrait s'installer plus en profondeur dans votre système
- Conservez les preuves : capture d'écran, photo avec votre téléphone
- Alertez votre service informatique si vous êtes dans le milieu professionnel
- Exécutez un scan par votre antivirus
- Nettoyez la source de l'infection (désinstallez le logiciel malveillant, ou autre persistance)

D'autre part, il existe ou existera peut-être un outil de déchiffrement pour le type de rançongiciel que vous avez subi. Pour vérifier cela, envoyez un de vos fichiers chiffrés sur No more Ransom.

N'oubliez pas d'effectuer régulièrement des sauvegardes hors ligne.
Cela vous permettra de vous en remettre plus rapidement.

==========

Pour plus d'informations / For more informations :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Day 16 - Ransomware
[EN]

A ransomware scam uses malicious software to lock your computer and make all your computer content inaccessible.
Then, the software demands a ransom for the recovery of the data or its non-divulgation on the internet, often with a countdown timer displayed on the screen.
This type of software appears when you install pirated software, or open a malicious attachment, file or link.

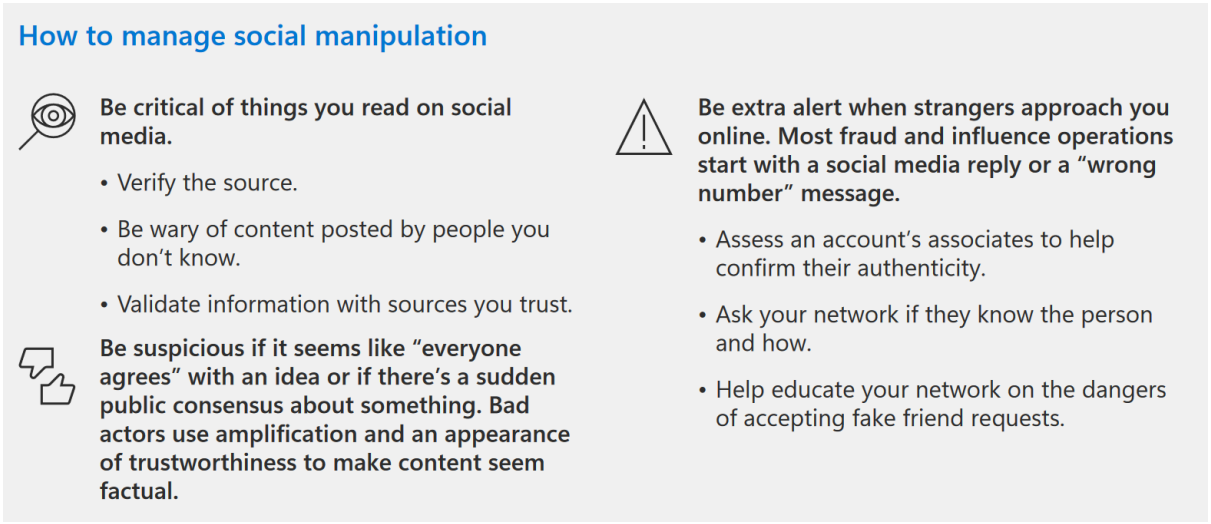
What should you do if you fall victim to this type of scam ?
Never pay ransom !
You won't be sure of recovering your data, and the malware may still be active on your equipment.

- Disconnect your equipment from the network (wired, wireless, shared connection).
- Don't turn off your equipment: the software could install itself deeper into your system.
- Keep proof : screenshots, photos taken with your phone
- Alert your IT department if you're in the workplace
- Run an antivirus scan
- Clean up the source of infection (uninstall the malware, or other persistence)

There is or may be a decryption tool for the type of ransomware you've suffered. To check this, send one of your encrypted files to No more Ransom.

Don't forget to make regular offline backups.
This will help you recover more quickly.

https://youtu.be/Wk9lTOCu1iU



Mercredi 23 octobre :

Jour 17 - Faux support technique / informatique
@tous [English version in the thread]

En visitant le prétendu site des impôts, vous recevez un message anxiogène indiquant une infection virale et demandant d'appeler **en urgence** un prétendu support technique « gratuit ».
En contactant le numéro, votre interlocuteur vous demande d'installer un logiciel de prise en main à distance pour qu'il puisse vous dépanner.
Lorsqu'il arrive à se connecter à votre poste, il installe un logiciel qui récupère tous vos mots de passe et données personnelles.

Aucun support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.
Personne, ni même votre service informatique professionnel ne vous demandera vos mots de passe.

Comment réagir ?

- Ne répondez pas aux sollicitations, et n'appelez jamais le numéro indiqué. D'autant qu'il est sûrement surtaxé.
- Si votre ordinateur semble "bloqué", redémarrez votre navigateur Internet. Cela suffit dans la plupart des cas à résoudre le problème
- Désinstallez toute nouvelle application suspecte
- Faites une analyse antivirale complète de votre appareil
- Signalez les faits sur la plateforme Pharos

Vous pouvez retrouver un cas pratique à réaliser sur la plateforme de formation Sens Cyber.

Lien vidéo du jour (Faux support technique du Sens Cyber de cybermalveillance.gouv)

Day 17 - Fake technical / IT support
[EN]

Visiting the so-called tax site, you receive an anxiety-inducing message indicating a viral infection and asking you to make **an emergency** call to so-called "free" technical support.
When you call the number, a person asks you to install remote control software so that he can help you out.
When he reach to connect to your workstation, he installs software that steal all your passwords and personal data.

No official technical support will ever contact you to ask for money.
No one, not even your professional IT department, will ever ask you for your passwords.

How to react ?

- Don't respond to solicitations, and never call the number given. Especially as it's

probably a premium-rate number.
- If your computer seems to be “blocked”, restart your Internet browser. In most cases, this will solve the problem.
- Uninstall any new suspicious applications
- Run a full antivirus scan on your device
- Report the incident to the Action Fraud platform.

You can find a case study on the French training platform Sens Cyber.

https://www.cybermalveillance.gouv.fr/medias/2024/02/240226_RA_2023_SCREEN.pdf
(page 35)

Jeudi 24 octobre :

Jour 18 - Piratage comptes
@tous [English version in the thread]

Vous avez remarqué une activité suspecte sur un de vos comptes ?
Vos contacts vous indiquent avoir reçu un message de votre part alors que vous n'en êtes pas l'auteur/l'émetteur ? Il s'agit peut-être de l'œuvre d'un pirate informatique qui accède à votre compte à votre insu. Comment réagir en cas de piratage, ou de suspicion ?

Tentez de vous connecter avec vos identifiants pour modifier votre mot de passe.
Si cela ne fonctionne pas, effectuez la procédure de "mot de passe oublié" pour pouvoir le changer par votre adresse mail principale, ou par votre numéro de téléphone.

Si votre boite mail "principale" a été piratée, cela est plus complexe.
Si vous arrivez à vous y connecter :

- **Changez immédiatement votre mot de passe**
- Renforcez la connexion à votre compte en activant la double authentification
- Vérifiez l'absence de règle de filtrage ou de redirection de vos messages
- Déconnectez de votre compte tout appareil ou session active inconnus
- Vérifiez que votre adresse mail, et votre numéro de téléphone de récupération soient les bons
- Changez tout les mots de passe de vos comptes et services rattachés à cette adresse mail
- Vérifiez qu'aucune publication ou commande n'a été réalisée
- Prévenez vos contacts afin qu'ils ne deviennent pas victimes des cybercriminels à leur tour
- Alertez votre banque et surveillez vos comptes bancaires à la recherche de toute transaction suspecte dont vous ne seriez pas à l'origine
- En fonction du cas d'espèce et du préjudice subi, vous pouvez déposer plainte sur la plateforme Thesee

=======

Votre boite mail "principale" est la plus critique pour vous, car elle peut permettre de se connecter à d'autres services qui lui sont rattachés si le pirate informatique effectue des procédures de "mot de passe oublié" par mail.

Si vous n'arrivez toujours pas à récupérer votre compte, contactez le service de messagerie concerné pour signaler votre piratage et demander la réinitialisation de votre mot de passe. Voir détail ici

=======

Pour plus d'informations / For more informations :

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/que-faire-en-cas-de-piratage-de-boite-mail
- https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

Day 18 - Hacked account
[EN]

Have you noticed suspicious activity on one of your accounts?
Your contacts told you they've received a message from you, even though you're not the author/sender ? This could be the work of a hacker accessing your account without your consent. What should you do if you suspect a hacker ?

Try logging in with your login details to change your password.
If this doesn't work, follow the "forgotten password" procedure to change it to your main email address or telephone number.

If your "main" mailbox has been hacked, this is more complicated.
If you manage to log in :

- **Change your password immediately**
- Enforce your account connection by activating double authentication.
- Check that there are no filtering or redirection rules for your messages
- Disconnect any unknown devices or active sessions from your account
- Check that your recovery email address and telephone number are correct
- Change all passwords for accounts and services linked to this email address
- Check that no publications or orders have been placed
- Warn your contacts so they don't fall victim to cybercriminals themselves
- Alert your bank and monitor your accounts for any suspicious transactions not originating from you
- Depending on the case and the damage suffered, you can file a complaint to the Action Fraud platform.

========

Your "main" mailbox is the most critical for you, as it can be used to log in to other related services if the hacker carries out "forgotten password" procedures by email.

If you still can't recover your account, contact the email service concerned to report your hack and request that your password be reset. See details here

Vendredi 25 octobre :

Jour 19 - Sensibilisation jeunes
@tous [English version in the thread]

Parce que vous aussi, vous pouvez être acteur dans la sensibilisation à la sécurité informatique en accompagnant vos enfants dans la compréhension des usages numériques.

Voici une playlist animé fort sympathique :
https://www.youtube.com/playlist?list=PLTsLW998ww7R-lpejSLj2hjo2BABO9CO3

Et quelques ressources interactives :
- De 7 à 11 ans : https://permisinternet.com/permiz/index.html
- De 11 à 14 ans : Cyber réflexes / Cyber guide famille
- Adolescent : Plateforme Sens Cyber / Pix

=========

Pour plus d'informations / For more informations :
- https://www.internet-signalement.gouv.fr/PharosS1/info/conseils/jeunes
- https://permisinternet.com/conseils-aux-parents/

- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/dossier-accompagnement-sensibilisation-des-jeunes
- https://www.internetsanscrainte.fr/ressources
- https://saferkidsonline.eset.com/

Day 19 - Youth awareness
[EN]

Because you too can be a part of awareness of IT security by helping your children to understand digital uses.

Here's a nice animated playlist :
https://www.youtube.com/playlist?list=PLibWTTXOV3uRQ2mqXoZL9AMSJ3_NWXEcb

And a few resources :
- https://www.cisa.gov/news-events/news/keeping-children-safe-online
- https://backgroundchecks.org/the-concerned-parents-toolbox-120-tools-and-tricks-to-protect-your-kids.html
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/

3018 : Cyber harcèlement et violences numériques
116 006 : France Victimes

Semaine 5

Lundi 28 octobre :

Jour 20 - Vérification des liens
@tous [English version in the thread]

Lors de votre navigation internet, on vous propose de vous rediriger vers un autre site, ou vous souhaitez installer un logiciel qu'on vous a recommandé, mais le lien vous parait bizarre.
Quelles sont les bonnes pratiques pour vérifier qu'un lien est bien légitime ?

Méthodes de base :

- Au moindre doute, ne cliquez pas.
- Cherchez manuellement le site sur votre moteur de recherche
- Consultez toujours le site officiel (vous pouvez le vérifier sur la page wikipédia du logiciel / site pour vérifier la bonne adresse)

Méthodes avancées :

- Passez votre souris sur le lien pour identifier vers où il vous redirigera
- Vérifiez l'orthographe du site s'il n'y a pas de faute ou de remplacement de lettre (Par exemple : impols guv.fr → impo**t**s.g**o**uv.fr)
- Utilisez un vérificateur d'URL : Google / Orange Cybersecure / VirusTotal (pouvant également analyser des fichiers vérolés)
- Évitez absolument les sites "répertoriant" tous les logiciels tels : softonic / 01.net / uptodown et autres. Ils ajoutent des publicités aux logiciels avant de les redistribuer

==========

Au passage, souvenez-vous que si vous installer un faux logiciel ou un logiciel piraté cela pourrait potentiellement :

- Installer d'autres applications, services, et utilitaires superflus
- Accéder à plus de fonctionnalités qu'il n'a besoin
- Transférer vos données sur un site externe
- Chiffrer votre PC
- Créer une porte d'entrée sur votre poste pour un futur attaquant

Day 20 - Link verification
[EN]

While you're surfing the web, someone suggests redirecting you to another site, or you want to install a piece of software that's been recommended to you, but the link seems odd.
What are the best practices for checking that a link is legitimate?

Basic methods :

- If in doubt, don't click.
- Search for the site manually on your search engine
- Always consult the official site (you can check on the wikipedia page of the software / site to verify the correct address)

Advanced methods :

- Hover your mouse over the link to identify where it will redirect you
- Check the spelling of the site for errors or letter replacements (e.g. nytlme com → nyt**i**me**s**.com)
- Use a URL checker: Google / Orange Cybersecure / VirusTotal (which can also analyze infected files)
- Absolutely avoid sites that “list” all software, such as softonic / 01.net / uptodown and others. They add advertisements to software before redistributing it.

=======

Remember, installing fake or pirated software could potentially :

- Install other unnecessary applications, services and utilities
- Access more functionality than it needs
- Transfer your data to an external site
- Encrypt your PC
- Create an entry point to your computer for a future attacker

Autres types d’arnaques :

- Typosquatting (remplacer des lettres dans l’adresse : lap0sle.net)
- Redirection de lien
    - Utiliser un déraccourcisseur d’url : https://unshorten.it/

Mardi 29 octobre :

Jour 21 - Ordinateur & réseaux wifi public
@tous [English version in the thread]

Utiliser un réseau WiFi public est risqué car il peut être contrôlé par une tierce personne qui pourrait intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire, etc.. et donc vous pirater votre compte.

C'est dans ce cadre là que l'utilisation d'un VPN est utile. Car il permet de chiffrer vos données sur le réseau auquel votre équipement est connecté. Empêchant le propriétaire du réseau de récupérer vos informations personnelles.

Si vous n'en n'avez pas, ou que vous vous connectez à un ordinateur en libre accès, évitez dans la mesure du possible de renseigner des informations sensibles ou personnelles sur un matériel ou un réseau qui n'est pas le vôtre.

Si vous y êtes contraint malgré tout, pensez à bien vous déconnecter de votre compte après utilisation pour empêcher que quelqu'un puisse y accéder après vous. Ainsi que de changer votre mot de passe lorsque vous le pourrez de nouveau.

D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent inutilement votre batterie.

Day 21 - Public wifi networks
[EN]

Using a public WiFi network is risky, because it can be controlled by a third party who could intercept your connections and, in the process, steal your access accounts, passwords, credit card data, etc., and thus hack into your account.

This is where a VPN comes in handy. It encrypts your data on the network to which your equipment is connected. Preventing the network owner from stealing your personal information.

If you don't have one, or if you're connecting to an open-access computer, avoid entering sensitive or personal information on equipment or a network that isn't your own.

If you are forced to do so, remember to log out of your account after use, to prevent anyone else from accessing it after you have. And change your password when you're able to do so again.

In general, disable all wireless connections when you're not using them (Wi-Fi, Bluetooth, NFC...), as they are all open doors to your device. What's more, they drain your battery unnecessarily.

Mercredi 30 octobre :

Jour 22 - Protection vie privée & RGPD
@tous [English version in the thread]

Dans un monde hyperconnecté, protéger sa vie privée en ligne, c'est avant tout protéger sa vie privée au quotidien.

Sur les réseaux sociaux :

- Optez pour un pseudo et une adresse mail non-nominative : simple mais efficace pour rester discret !
- Cloisonnez vos usages en fonction de votre audience : pas besoin que tout le monde sache tout.
- Limitez l'audience de vos publications et de votre profil pour garder un contrôle sur ce que vous partagez.
- Faites régulièrement le ménage dans les applications tierces connectées à votre compte pour éviter de partager vos infos sans le vouloir !

Et au quotidien ?

- Remplissez le strict minimum sur les formulaires en ligne : pour acheter un produit, pas besoin de renseigner votre âge, votre date de naissance, ou votre statut familial !
- Masquez votre adresse email et votre numéro de téléphone lors des inscriptions et annonces en ligne : un bon moyen d'éviter les spams et appels frauduleux !

⚖️ Et pour vos droits ? En Europe, le RGPD (Règlement Général sur la Protection des Données) veille sur la gestion de vos données personnelles. Il vous donne des droits précieux : Information, Accès, Rectification, Opposition, Limitation, Extraction, et même la suppression de vos données !
Tout savoir ici 👉
https://www.cnil.fr/fr/mes-demarches/les-droits-pour-maitriser-vos-donnees-personnelles

Quelques outils pour sécuriser votre navigation 🛠️

- uBlock Origin : pour bloquer les pubs envahissantes.
- Privacy Badger ou Ghostery : deux excellents bloqueurs de trackers pour rester discret en ligne.

Enfin, voici une petite vidéo pour aller plus loin 🎥
https://youtu.be/wulsmoi7LuM

Avec ces conseils, vous voilà un peu plus armé pour surfer en toute sérénité !

========

Pour plus d'informations :

- https://www.cnil.fr/fr/4-reflexes-pour-mieux-proteger-votre-identite-en-ligne
- https://www.cnil.fr/fr/10-conseils-pour-rester-net-sur-le-web
- Pour porter plainte sur un sujet en lien avec vos données personnelles : https://www.cnil.fr/fr/plaintes

Day 22 - Privacy & RGPD
[EN]

Today in a hyper-connected world, protecting your privacy online means protecting your privacy on a daily basis.

On social networks :
- Use a pseudonym and a non-nominative e-mail address : simple but effective way to keep a low profile !
- Separate your uses according to your audience: there's no need for everyone to know everything.
- Limit the audience for your publications and your profile to keep control over what you share.
- Regularly clean up the third-party applications connected to your account to avoid sharing your information unintentionally !

And in everyday life?
- Fill in the bare minimum on online forms : to buy a product, there's no need to fill in your age, birthday, or family status !
- Hide your email address and phone number when registering and advertising online: a good way to avoid spam and fraudulent calls !

⚖️ What about your rights ? In Europe, the GDRP (General Data Protection Regulation) oversees the management of your personal data. It gives you valuable rights: Information, Access, Rectification, Opposition, Limitation, Extraction, and even Deletion of your data! Find out all about it here 👉 https://www.cnil.fr/en/gdpr-toolkit

Some tools to secure your browsing 🛠️
- uBlock Origin : to block invasive ads.
- Privacy Badger or Ghostery : two excellent tracker blockers to stay discreet online.

Finally, to end the day on a high note, here's a little video to take you further 🎥
https://youtu.be/wulsmoi7LuM

With these tips, you're all set to surf with peace of mind ! 🚀

========

For more informations :
- https://www.cnil.fr/en/discover-incollables-2020-quiz-privacy-challenge-each-other-and-showing-your-knowledge-data

Plus d'outils :
- https://respectemesdatas.fr/
- https://justdeleteme.xyz

Jeudi 31 octobre :

Jour 23 - Conclusion
@tous [English version in the thread]

Nous y voilà, le dernier jour.
J'espère que nous ne vous avons pas fait trop peur avec tous ces messages.

Utilisez tout ce que vous avez pu apprendre ici comme une boîte à outils qui vous permettra de réagir en cas de besoin aux différentes situations auxquelles vous pourrez être confrontés dans le futur.
Un PDF de récap de tous les messages est disponible ci-joint.
Parce que la sensibilisation à la sécurité informatique est d'intérêt public, vous êtes libre de partager ceci autour de vous pour concevoir et améliorer votre propre boîte à outils.

Évidemment, tous les sujets n'ont pas été évoqués, vous n'aurez pas tout retenu, ou tout compris totalement, mais le principal est de s'améliorer de façon continue.

Vu avec certains d'entre-vous, nous essayerons par la suite de faire des présentations plus concrètes et détaillées sur un sujet précis de temps en temps.

Pour terminer, voici un récapitulatif du site de référence et des plateformes de sensibilisations :

- **https://www.cybermalveillance.gouv.fr/bonnes-pratiques**
- https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre
- https://pix.fr/
- https://secnumacademie.gouv.fr/

En cas de besoin, pour diagnostiquer un problème :
https://www.cybermalveillance.gouv.fr/accueil-assistance

Qu'en avez-vous pensé ? Qu'avez-vous appris ? Avez-vous des améliorations, des suggestions ?
N'hésitez pas à nous faire part de vos retours dans le fil de discussion.

Merci à tous pour votre écoute.

Le service IT

Day 23 - Conclusion
[EN]

Here we are, the last day.
I hope we haven't scared you too much with all these messages.

Use everything you've learned here as a toolbox to help you with any situations in the future.
A PDF with all the messages is attached.
Because IT security awareness is important, please feel free to share this with others to improve your own toolbox.

Obviously, not every topic has been covered, and you won't have retained everything, or understood everything completely, but the main thing is to keep improving.

In view of the discussions we've had with some of you, we'll try to make more concrete and detailed presentations on a specific subject later.

To conclude, here's a summary of the reference site and awareness platforms:

- **https://www.cybermalveillance.gouv.fr/bonnes-pratiques**
- https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre
- https://pix.fr/
- https://secnumacademie.gouv.fr/

If you need to diagnose a problem :
https://www.cybermalveillance.gouv.fr/accueil-assistance

What did you think ? What did you learn ? Do you have any suggestions for improvement ?
Don't hesitate to give us your feedback in the discussion thread.

IT Service