

CYBERSÉCURITÉ

UN GUIDE DE BONNES PRATIQUES

Thales Media Day, 31 mai 2022

#Cybersécurité : nouvelles menaces et nouveaux enjeux

...

THALES
Building a future we can all trust

PRÉSENTATION

En 2021, les **cas de ransomware** ont augmenté de 435 %, classant la **cybersécurité** parmi les dix principaux risques auxquels le monde est confronté. Aujourd'hui, la cybersécurité et ses enjeux sont devenus une réalité opérationnelle pour les **entreprises et les organisations gouvernementales**, et une préoccupation croissante pour les **particuliers**.

La priorité doit être donnée à la détection des menaces - le plus rapidement possible - et à la limitation de leurs effets les plus graves : vol ou corruption de données et dommage sur les systèmes d'information.

À L'OCCASION DES

#ThalesMediaDay...

Veillez à adopter les bons réflexes

Nous pouvons tous mieux anticiper, détecter et prévenir les cybermenaces.



Anticiper

Comment se prémunir des **cyberattaques** sur les appareils électroniques ?

> Soyez attentif au « phishing »

C'est-à-dire aux mails frauduleux vous demandant des informations sensibles ou vous incitant à télécharger des logiciels malveillants, en particulier lorsque vous effectuez des achats en ligne.

> Utilisez un mot de passe unique et complexe

Pour garantir une sécurité maximale : choisissez le mot de passe le plus long, le plus insolite, le **plus fort** possible.

> Utilisez un réseau privé virtuel (VPN) de confiance

Dans la mesure du possible, et notamment lorsque vous utilisez des réseaux Wi-Fi gratuits.

> Faites attention à votre empreinte numérique

C'est-à-dire aux informations personnelles et professionnelles que vous partagez en ligne.

> Activez les services d'authentification à deux facteurs

De nombreux sites Web proposent ces services afin de renforcer la sécurité et garantir ainsi que vous êtes le seul à pouvoir accéder à vos comptes.



Détecter et prévenir

#1

La navigation sur le web...

SOULÈVE DES PROBLÈMES DE CONFIDENTIALITÉ



Pièges à clics, publicités, téléchargements illégaux, navigateurs web sécurisés ou non...



COMMENT SE PROTÉGER ?

- se familiariser avec les paramètres de confidentialité des navigateurs et les régler (modes privé, incognito, inprivate)
- effacer les données de navigation (cookies, etc)
- refuser le partage des données

#2

Les courriers électroniques...

SOULÈVENT DES PROBLÈMES DE SÉCURITÉ



Arnaques, spams, origine des mails...



COMMENT SE PROTÉGER ?

Créer des règles dans la boîte mail :

- à partir de mots ou d'expressions pour permettre un meilleur contrôle du filtrage
- pour configurer des déclencheurs d'alerte
- pour éviter de recevoir du courrier indésirable

#3

Les logiciels malveillants...

SOULÈVENT DES PROBLÈMES D'INFECTION



Pièges à clics, publicités, téléchargements illégaux, navigateurs web sécurisés ou non...



COMMENT SE PROTÉGER ?

- renforcer les paramètres de l'ordinateur
- vérifier si une application ou un fichier prend plus de mémoire qu'il ne le devrait
- vérifier les performances du système

#4

Les médias sociaux et l'usurpation d'identité...

SOULÈVENT DES PROBLÈMES DE SÉCURITÉ



Achats frauduleux en ligne, faux appels, vol de données...



COMMENT SE PROTÉGER ?

Pour rester en sécurité :

- sachez que, s'il ne faut que quelques secondes pour poster, votre publication laisse des traces indélébiles
- gardez à l'esprit que votre niveau de vie privée est intrinsèquement lié aux informations que vous publiez
- ne partagez jamais aucun détail sur votre localisation
- n'autorisez l'accès qu'aux applications auxquelles vous faites confiance
- méfiez-vous de vos nouveaux amis en ligne ou partenaires amoureux potentiels

#5

Les smartphones...

SOULÈVENT DES PROBLÈMES DE SÉCURITÉ



Téléchargement d'applications, autorisations de téléchargement, quantité de données personnelles disponibles, faux appels...



COMMENT SE PROTÉGER ?

- faites attention à ce que vous partagez
- faites attention aux arnaques par SMS
- faites preuve de bon sens vis-à-vis de vos données personnelles
- vérifiez le nom du destinataire avant d'envoyer un message
- utilisez un écran de verrouillage ou un code PIN pour plus de sécurité

#6

Les mots de passe...

SOULÈVENT DES PROBLÈMES DE CONFIDENTIALITÉ



COMMENT SE PROTÉGER ?

- mémorisez vos informations de connexion
- utilisez une authentification multifactorielle
- autorisez les gestionnaires de mots de passe à utiliser des mots de passe forts
- prenez l'habitude d'utiliser des caractères spéciaux
- n'utilisez pas les mêmes mots de passe

Thales Media Day, 31 mai 2022

*#Cybersécurité : nouvelles menaces
et nouveaux enjeux*

Contacts Relation médias chez Thales

Chrystelle Dugimont :

+33 6 25 15 72 93

(chrystelle.dugimont@thalesgroup.com)

Marion Bonnet :

+33 6 60 38 48 92

(marion.bonnet@thalesgroup.com)

Inès Samama :

+33 7 82 36 32 79

(ines.samama@thalesgroup.com)

www.thalesgroup.com