J'améliore ma cybersécurité

Comportements clefs pour éviter les plus grands risques

Je prends soin de mes accès

- ✓ J'ai un mot de passe différent sur chaque site, de plus de 12 caractères, impossible à deviner
- ✓ Donc j'utilise un gestionnaire de mots de passe reconnu
- ✓ J'active la double authentification (2FA) dès que possible

Mon email est mon pire ennemi

- ✓ Est suspect tout email d'origine inconnue ou que je n'attendais pas
- ✓ Je n'ouvre jamais de pièce jointe d'un email suspect
- ✓ J'évite de suivre un lien inclus dans un email suspect

Mes secrets & données sont à moi seul.e

- ✓ Je ne partage ni mot de passe, ni carte de crédit, ni code PIN, ...
- ✓ Je ne réponds jamais à une demande d'info que je n'attendais pas
- ✓ Je n'utilise pas de wifi non protégé, mes données y sont en danger

Mes appareils sont des forteresses

- ✓ Je verrouille tous mes appareils dès que je m'en éloigne
- ✓ Je maintiens à jour mon système d'exploitation, antivirus & gestionnaire de mots de passe
- ✓ J'évite les clefs USB (et apparentés)

Par défaut je doute, sauf si j'ai bien vérifié

- ✓ Je sais que "si c'est trop beau pour être vrai, ce n'est pas vrai"
- ✓ Je redouble de prudence au moindre doute
- ✓ Je vérifie toute information choquante, effrayante, émouvante

Editeur responsable: Enspirit SRL — Version 1.1, Janvier 2023 — Distribué sous licence creative commons — Infos & contributions: info@enspirit.be

J'améliore ma cybersécurité

Situations dangereuses, à améliorer immédiatement

Mots de passe

- ✓ Un mot de passe utilisé sur plusieurs sites web et non changé depuis 2 ans est compromis.
- ✓ Il est connu dans les bases de données du dark web.
- ✓ Il faut le changer d'urgence.

Virus

- ✓ Un ordinateur de bureau avec accès Internet et sans antivirus est compromis.
- ✓ La présence d'un virus ou d'un trojan est plus que probable.
- ✓ Il faut, à minima, installer un antivirus et scanner la machine immédiatement.

Phishing

- ✓ Un collaborateur qui n'a jamais entendu parler formellement des cyber-risques est compromis.
- ✓ La probabilité qu'il ou elle soit victime d'une tentative de phishing est immense.
- ✓ Il faut, à minima, sensibiliser aux principaux risques cyber pour l'aider à reconnaître les situations dangereuses.

Backups et Plans de reprise

- ✓ Les backups et plans de reprises inexistants et/ou non testés sont compromis.
- ✓ La probabilité de ne pas pouvoir relancer l'entreprise est grande.
- ✓ Il faut, à minima, créer ces plans et backups et les tester régulièrement.

Editeur responsable: Enspirit SRL — Version 1.1, Janvier 2023 — Distribué sous licence creative commons — Infos & contributions: info@enspirit.be