DELL Technologies

Aide-mémoire sur la cybersécurité

La cybercriminalité connaît actuellement un essor fulgurant, ce qui n'est pas surprenant dans un monde de plus en plus virtuel. En effet, **les cyberattaques ont généré environ 6 000 milliards de $ en 2021**, devenant ainsi la troisième économie mondiale, juste derrière les États-Unis et la Chine* ! S'il est vrai que les pirates élaborent des attaques de plus en plus intelligentes et sophistiquées, il est facile de se protéger en ligne en se renseignant sur les menaces les plus récentes et en adoptant des mesures de protection. **Voici quelques-unes des menaces que les experts en cybersécurité de Dell s'efforcent de neutraliser, ainsi que des conseils pour protéger votre lieu de travail et votre foyer.**

Attaque par opportunisme

Des utilisateurs malveillants accèdent à votre système lorsque vous visitez un site Web non sécurisé ou compromis.

Les indices à repérer :

Nouveaux fichiers ou nouvelles connexions réseau ajoutés sur votre système sans que vous en soyez à l'origine

Demandes spontanées d'informations de configuration

ASTUCE : *Mettez systématiquement à jour vos navigateurs et plug-ins.*

Votre connexion n'est pas sécurisée.

Matériel non sécurisé

ASTUCE : *Effectuez vos achats auprès de vendeurs agréés.*

Saviez-vous que votre imprimante pouvait être piratée ?

Les acteurs malveillants introduisent des failles de sécurité dans le matériel et les accessoires.

Les indices à repérer :

Offres trop belles pour être vraies

Ingénierie sociale

Les escrocs se font passer pour une entité légale ou un organisme officiel afin de voler des **informations personnelles ou financières** sensibles (également connu sous le nom de « phishing »). Le code malveillant est envoyé sous forme de lien ou de pièce jointe par e-mail, messagerie instantanée ou SMS.

Les indices à repérer :

E-mails ou SMS spontanés demandant de saisir des informations personnelles et redirigeant vers des pièces jointes ou une ouverture de lien

Adresse e-mail d'expéditeur, formulation et orthographe douteuses

ASTUCE : *Les administrations (DGFP et autres) vous contacteront toujours d'abord par courrier.*

Serait-ce une tentative de phishing ?

Attaque par logiciel malveillant sur USB

ASTUCE : *Méfiez-vous des clés USB inconnues, même si elles proviennent de proches.*

Puis-je vraiment insérer cette clé USB sans risque ?

Les cybercriminels utilisent des périphériques de stockage amovibles, comme des clés USB, des disques durs portables, des smartphones, des lecteurs audio, des cartes SD ou des supports optiques (CD, DVD, Blu-Ray), pour infecter un ordinateur ou un réseau.

Les indices à repérer :

Accès inattendu à des fichiers ou nouveaux fichiers créés sur l'appareil

Relation de confiance

Les pirates compromettent un tiers de confiance, comme un cabinet médical, et utilisent sa réputation pour profiter des patients.

Les indices à repérer :

Comportement de connexion inhabituel

ASTUCE : *Utilisez des mots de passe forts et uniques.*

Qui êtes-vous ?

Comment se protéger en ligne :

Ce qu'il faut faire

Utilisez l'authentification multifacteur ainsi que des mots de passe forts et uniques pour vos différents comptes.

Tout appareil connecté à internet peut faire l'objet d'une attaque. Mettez systématiquement à jour vos logiciels.

Soyez attentif et vigilant. Apprenez à reconnaître les techniques d'escroquerie.

Signalez tout incident à l'équipe IT, et avertissez vos collaborateurs et vos proches.

Ce qu'il ne faut pas faire

Ne soyez pas négligent. Suivez à la lettre tous les protocoles de sécurité.

Ne cliquez pas sur les liens contenus dans des e-mails ou des messages instantanés spontanés.

N'ignorez pas les avertissements émis par votre navigateur, tels que « Votre connexion n'est pas sécurisée » ou « Votre connexion n'est pas privée ».

ASTUCE : *Pour en savoir plus, rendez-vous sur :* Dell.com/Endpoint-Security.

DELL Technologies

*Cybersecurity Ventures: 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics