Pistagnesi Maison d'expertise en souscription

420, boul. Charest Est, bur. 330
Québec (Québec) G1K 8M4

T. 418 523-4000
Sans frais 1 877 523-4001

pistagnesi.com

Formation - Cybersécurité

Chez Pistagnesi, la cybersécurité est une priorité stratégique. Cette formation de sensibilisation a pour but d'aider chaque employé à développer de bons réflexes face aux cybermenaces et à protéger nos systèmes, nos données et nos clients.

OBJECTIFS DE LA FORMATION

- Comprendre les principales menaces en cybersécurité
- Adopter les bons réflexes numériques au quotidien
- Favoriser une culture de vigilance et de collaboration autour de la sécurité

THÈMES ABORDÉS

- Hameçonnage
- Virus et rançongiciels
- Mots de passe
- Authentification multifactorielle (MFA)
- Sécurité des appareils mobiles
- Sécurité Wi-Fi
- Ingénierie sociale

HAMEÇONNAGE

Le hameçonnage (phishing) est une tentative de fraude par courriel, texto ou message instantané visant à vous inciter à cliquer sur un lien ou à fournir des renseignements personnels.

Bonnes pratiques :

- Vérifiez toujours l'expéditeur avant de cliquer.
- Méfiez-vous des messages urgents ou menaçants.
- Ne fournissez jamais d'informations personnelles par courriel.
- Signalez immédiatement tout courriel suspect à l'équipe TI.

Saviez-vous que : plus de 80 % des cyberattaques commencent par un courriel de phishing.

P.

VIRUS ET RANÇONGICIELS

Un rançongiciel (ransomware) chiffre vos données et exige une rançon pour les débloquer. Les virus, eux, peuvent voler, détruire ou bloquer des informations sensibles.

Bonnes pratiques :

- N'ouvrez jamais de pièces jointes non sollicitées.
- Survolez les liens pour vérifier l'adresse avant de cliquer.
- Maintenez vos logiciels et antivirus à jour.
- Sauvegardez régulièrement vos données sur un support sécurisé.

Saviez-vous que : payer une rançon ne garantit jamais de récupérer vos données.

MOTS DE PASSE

Les mots de passe sont la première barrière de protection. Les anciennes recommandations de changer son mot de passe tous les 3 mois ne sont plus valables. Aujourd'hui, l'important est d'utiliser des mots de passe longs, uniques et complexes.

Bonnes pratiques :

- Créez des mots de passe d'au moins 12 caractères.
- Utilisez un mélange de lettres, chiffres et symboles.
- Ne réutilisez jamais le même mot de passe sur plusieurs comptes.
- Utilisez un gestionnaire de mots de passe pour les conserver en sécurité.

Saviez-vous que : un mot de passe de 8 caractères peut être piraté en quelques minutes, tandis qu'un mot de passe de 12 caractères alphanumériques prendrait des années.

AUTHENTIFICATION MULTIFACTORIELLE (MFA)

L'authentification multifactorielle ajoute une deuxième couche de protection. Même si votre mot de passe est compromis, un pirate ne pourra pas accéder à vos comptes sans la deuxième étape.

Bonnes pratiques :

- Activez la MFA partout où elle est disponible.
- Utilisez de préférence une application d'authentification (Google Authenticator, Microsoft Authenticator) ou une clé physique (Yubikey) plutôt qu'un simple SMS.

Saviez-vous que : la MFA bloque plus de 99 % des tentatives de piratage liées aux mots de passe.

P.

SÉCURITÉ DES APPAREILS MOBILES

Les téléphones et tablettes contiennent autant de données sensibles que les ordinateurs. Ils sont une cible privilégiée pour les cybercriminels.

Bonnes pratiques :

- Activez un code de déverrouillage et le verrouillage automatique.
- Désactivez Wi-Fi et Bluetooth quand vous ne les utilisez pas.
- Installez uniquement des applications provenant de sources officielles.
- Mettez à jour régulièrement vos appareils et applications.
- Ne partagez pas d'informations sensibles par texto.

Saviez-vous que : plus de 60 % des cyberattaques ciblent aujourd'hui les appareils mobiles.

SÉCURITÉ WI-FI

Les réseaux Wi-Fi publics gratuits et non sécurisés sont des portes d'entrée pour les pirates. Ils peuvent intercepter vos communications et voler vos données.

Bonnes pratiques :

- N'utilisez jamais un Wi-Fi public pour accéder à des données sensibles.
- Utilisez un VPN si vous devez absolument vous connecter à un réseau public.
- Assurez-vous que votre Wi-Fi personnel est protégé par un mot de passe fort et du WPA2 ou WPA3.

Saviez-vous que : un pirate peut créer un faux réseau Wi-Fi avec un nom familier pour piéger les utilisateurs.

INGÉNIERIE SOCIALE

L'ingénierie sociale est l'art de manipuler une personne pour lui soutirer des informations ou lui faire commettre une erreur. Elle peut prendre la forme d'appels téléphoniques, de faux profils sur les réseaux sociaux ou d'objets piégés laissés dans un lieu public.

Bonnes pratiques :

- Vérifiez toujours l'identité des personnes avant de partager des informations.
- Ne branchez jamais de clés USB trouvées dans des lieux publics.
- Méfiez-vous des demandes inhabituelles, même si elles semblent provenir d'un collègue ou d'un supérieur.

P.

Saviez-vous que : la majorité des attaques réussies reposent sur l’erreur humaine et non sur une faille technique.

RÉSUMÉ DES BONNES PRATIQUES

- Utilisez des mots de passe longs, uniques et complexes.
- Activez la MFA partout où c’est possible.
- Soyez vigilants face aux courriels suspects.
- N’ouvrez pas de pièces jointes ou liens douteux.
- Mettez à jour vos logiciels et appareils.
- Sauvegardez régulièrement vos données.
- Utilisez des réseaux sécurisés.
- Signalez toute activité suspecte à l’équipe TI.