CYBER READINESS
INSTITUTE

Préparation au numérique Conseils & Principes

La plupart des entreprises sont dotées de règles de base que tous les employés doivent suivre, par exemple arriver au travail à l'heure, quelle tenue porter au bureau ou comment demander des congés. Des directives générales concernant la préparation au numérique devraient également être incluses. Après tout, **la sécurité de vos données et de vos systèmes a un impact considérable sur votre entreprise et vos clients.** Nous vous recommandons de suivre les instructions et les conseils suivants pour informer vos employés et responsabiliser tous les membres du personnel afin de **créer une culture de la préparation au numérique.**

Mots de passe

Un mot de passe fort est essentiel pour sécuriser vos comptes et systèmes. Que ce soit pour accéder à des e-mails professionnels, récupérer des fichiers sur un disque dur partagé ou vous connecter à n'importe quel service en ligne, le mot de passe, ou la *phrase secrète*, que vous utilisez est important. Vous pouvez même ajouter une autre couche de sécurité avec l'authentification à deux facteurs. Cette dernière vous oblige à entrer un code unique envoyé sur votre appareil mobile à chaque nouvelle connexion. L'authentification à deux facteurs permet de créer un lien de sécurité important entre le mot de passe et la personne.

Nous vous encourageons à faire suivre ces consignes à vos employés :

1. Utilisez une phrase secrète longue qui contient des caractères spéciaux. Par exemple, une phrase de votre chanson, série ou film préféré.

2. N'utilisez jamais la même phrase secrète pour vos comptes professionnels et privés, et ne divulguez vos identifiants et mots de passe à personne, pas même vos collègues.

3. Utilisez l'authentification à deux facteurs à chaque fois que c'est possible.

Mises à Jour

Garder vos logiciels et vos systèmes d'exploitation à jour est crucial.
Chaque mise à jour de votre fournisseur de logiciel peut contenir des correctifs importants pour protéger votre logiciel et vos systèmes contre les attaques. Un grand nombre d'entreprises nomment une personne en charge des mises à jour pour tous les systèmes de la société, ce qui est préférable. Il est aussi possible de demander à chaque employé d'effectuer ses propres mises à jour. Dans tous les cas, des mises à jour régulières sont cruciales.

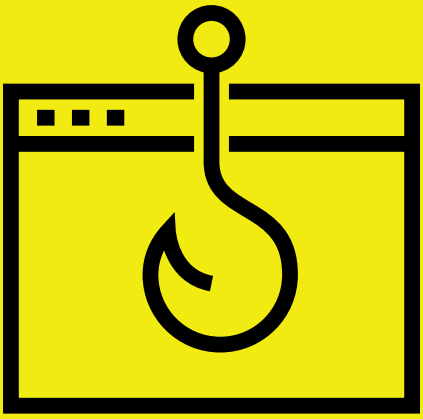
Nous vous recommandons de suivre ces instructions concernant les mises à jour:

1. Lorsque c'est possible, activez les mises à jour automatiques pour tous les équipements et tous les logiciels.

2. Mettez régulièrement à jour l'ensemble des vos systèmes d'exploitation, ordinateurs, téléphones et tablettes dès que vous êtes informés de la disponibilité d'une mise à jour.

3. Mettez à jour tous les logiciels et toutes les applications que ce soit ceux de l'entreprise ou ceux téléchargés par l'employé.

Phishing



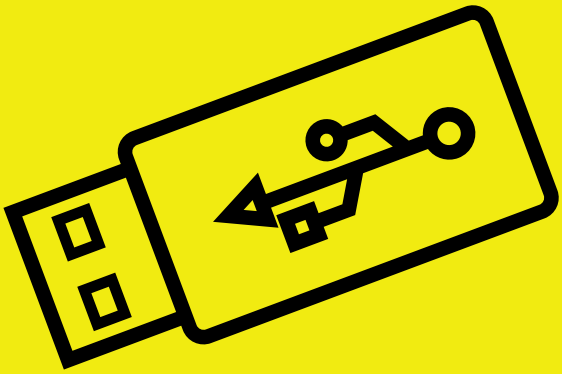
Le phishing est l'une des menaces les plus grandes et les plus communes du monde numérique aujourd'hui. Un e-mail de phishing a souvent l'air d'un message authentique et sûr. Néanmoins, son ouverture peut entraîner le téléchargement de virus ou donner accès à vos données à des pirates. Tout le monde reçoit des e-mails de phishing, c'est pourquoi il est important de bien savoir les reconnaître. Être prudent est la meilleur façon de se protéger.

Voici quelques conseils pour vous aider:

1. **Vérifiez que l'adresse de l'expéditeur et les autres informations d'identification comme le logo, l'adresse et le contact ne contiennent pas d'incohérences ou de signes montrant qu'ils ont pu être falsifiés.**

2. **Si l'adresse de l'expéditeur vous est inconnue, ne cliquez sur aucun lien et ne téléchargez aucune pièce jointe.**

3. **Supprimez tous les e-mails suspects et videz immédiatement votre corbeille.**



Clés USB & supports amovibles

Les clés USB sont pratiques pour partager des fichiers, mais elles peuvent aussi transmettre virus et malwares. Il n'y a aucun moyen de savoir d'où vient un support amovible et qui peut l'avoir infecté. La meilleure façon de prévenir les risques liés aux clés USB et aux supports amovibles consiste à en proscrire l'utilisation. Néanmoins, en interdire l'usage peut s'avérer difficile.

C'est pourquoi nous recommandons de suivre ces instructions :

1. Introduisez des alternatives aux clés USB, comme les services de partage sur le cloud, afin de réduire le besoin en supports amovibles.

2. Installez un ordinateur qui n'est pas connecté au réseau de l'entreprise afin d'analyser si les clefs USB sont infectées et d'effacer les données qui y sont présentes.

3. Faites preuve de bon sens, c'est important. Si vous ne connaissez pas l'origine d'une clé USB, ne la connectez à aucun appareil.

Réponse à un Incident

La préparation au numérique consiste à entreprendre les bonnes démarches pour réduire le risque, mais aussi à être prêts en cas d'incident. Mettre en place un plan de réponse aux incidents est une étape cruciale pour se préparer au numérique. Voyez cela comme un exercice d'incendie : si un incident a lieu, il est important d'avoir un plan dans lequel tout le monde connait son rôle.

Vous trouverez plus d'informations sur la réponse aux incidents dans le Cyber Readiness Program, mais vous pouvez déjà vous concentrer sur les trois points suivants :

1. Se préparer : Assurez-vous que les employés effectuent des sauvegardes régulières de leur travail et de leurs données.

2. Faire face : Si une attaque a lieu ou un problème se pose, déconnectez immédiatement du réseau l'équipement concerné. Tous les employés devraient suivre cette consigne.

3. Récupérer : Restaurez vos données à partir d'une sauvegarde et servez-vous de l'incident comme une expérience afin de renforcer les principes de préparation au numérique comme la sécurité des mots de passe, les mises à jour, la sensibilisation au phishing et la sécurité liée aux supports amovibles.

ÊTES-VOUS PRÊTS À PASSER AU NIVEAU SUIVANT ?

EXPLOREZ LE CYBER READINESS PROGRAM

Le Cyber Readiness Program est une ressource en ligne gratuite qui décrit les étapes pratiques que vous devez suivre pour évaluer et améliorer votre préparation au numérique. Facile à utiliser et permettant de suivre votre progression, vous pouvez travailler à votre rythme. Une fois terminé, vous recevrez un certificat de préparation au numérique pour montrer à vos clients et à vos fournisseurs que vous avez pris des mesures afin de créer une culture de la préparation au numérique au sein de votre organisation.

Pour en savoir plus :

https://www.cyberreadinessinstitute.org/the-cyber-readiness-program