Garantir la sécurité de votre organisation en ligne

Importance de la cybersécurité pour les groupes et les organisations communautaires

Cette page contient des conseils et quelques mesures que vous pouvez prendre pour protéger votre groupe ou organisation communautaire contre les menaces de cybersécurité. Il existe également un guide distinct pour les particuliers pour utiliser Internet en toute sécurité.

Ces conseils visent les menaces les plus courantes et les plus graves.

- Mises à jour – mettez les logiciels de vos appareils à jour pour corriger les éventuelles failles de sécurité.
    - Effectuez les mises à jour sur les appareils de votre groupe ou de votre organisation communautaire. Cela inclut les téléphones, les ordinateurs, les routeurs WiFi et tout ce qui se connecte à Internet, y compris les appareils intelligents.
    - Si possible, utilisez des mises à jour automatiques.
- Double authentification (2FA) : ajoute une sécurité supplémentaire à vos comptes en exigeant un mot de passe et une étape supplémentaire, comme un code provenant d'une application sur votre téléphone.
    - Remarque : cette procédure peut également être désignée comme étant, parmi bien d'autres noms, une authentification multifacteurs ou une vérification en deux étapes.
    - Activez la double authentification sur tous les comptes de votre groupe ou organisation communautaire.
    - Si possible, essayez d'utiliser une forme de 2FA résistante au phishing, afin de ne pas être induit à la révéler par la ruse. Cette couche supplémentaire de sécurité peut être une clé de sécurité physique, une empreinte digitale ou la reconnaissance faciale.
- Contrôlez vos comptes en ligne - vérifiez que les anciens membres n'ont plus accès aux comptes après avoir quitté le groupe ou l'organisation communautaire.
    - Si plusieurs personnes accèdent au même compte, assurez-vous qu'elles ont toutes des identifiants différents et que la double authentification est activée.
    - Établissez une liste de tous les comptes d'utilisateur et désactivez ceux qui ne sont pas nécessaires, par exemple lorsqu'une personne démissionne.
    - Tenez un registre de tous les appareils que vous avez donnés à vos membres et n'oubliez pas de les récupérer et de les réinitialiser si une personne quitte l'organisation. Vous devrez éventuellement modifier les codes d'accès physiques aux bâtiments.
- Vérifiez qui peut accéder à vos comptes en ligne : les membres de votre groupe ou organisation communautaire ne doivent avoir accès qu'aux éléments dont ils ont besoin.
    - Si le compte d'une personne est piraté, ces mesures permettent de limiter les préjudices possibles.

- Vérifiez et supprimez régulièrement les autorisations inutiles.
- Si vous n'utilisez qu'un seul compte administrateur auquel de multiples personnes ont accès, surveillez-le pour détecter toute activité inhabituelle. Essayez de limiter ce type de compte, en particulier pour les tâches quotidiennes.
- Ces règles s'appliquent également à l'accès administrateur aux appareils, tels que les routeurs.

- Examinez les contrats avec vos prestataires de services, si vous avez sous-traité vos services informatiques.
  - Vérifiez que des mesures de cybersécurité sont en place pour répondre aux besoins de votre groupe ou organisation communautaire.
- Comprenez les interactions entre tous vos comptes et tous vos systèmes ; comprendre les connexions vous aide à savoir où un attaquant est susceptible de s'infiltrer.
  - Examinez les connexions entre vos systèmes, par exemple, les plateformes de messagerie, de stockage en nuage et de comptabilité.
  - Envisagez le recours à un réseau privé virtuel (VPN) pour une sécurité en ligne accrue. L'utilisation d'un VPN masque votre activité en ligne à tous ceux qui pourraient essayer de vous suivre. Ce système est particulièrement utile pour les membres de votre groupe ou organisation communautaire qui se connectent à distance.
- Formez vos équipes ; les membres de votre groupe ou organisation communautaire sont plus susceptibles d'être ciblés que les systèmes.
  - Mettez en place une formation de base à la cybersécurité. Le site Internet Maîtrisez votre vie en ligne Own Your Online | NCSC propose un large éventail de conseils et d'astuces pour vous aider à vous protéger en ligne et à repérer les escroqueries.
  - Rappelez à vos équipes que ces conseils et astuces sont importants pour protéger leurs comptes personnels ainsi que ceux qu'ils utilisent pour leur organisation.
  - Nous avons également élaboré un guide s'adressant aux individus pour leur permettre d'assurer leur sécurité en ligne.
- Préparez-vous aux incidents éventuels ; il est nécessaire de mettre en place un plan pour éviter les situations de panique en cas d'incident.
  - Un plan d'intervention décrit les rôles et responsabilités en cas d'incident. Des modèles sont disponibles ici Incident Management | NCSC
  - Incluez un plan en cas de panne des systèmes téléphoniques, informatiques ou autres. Gardez ce plan à jour.
  - Conservez les coordonnées de toutes les personnes requises et leurs coordonnées de secours si le principal moyen de les contacter ne fonctionne plus (comme l'e-mail).
  - Conservez ce plan en dehors de votre système au cas où vous ne pourriez pas y accéder.