DIGITAL SECURITY

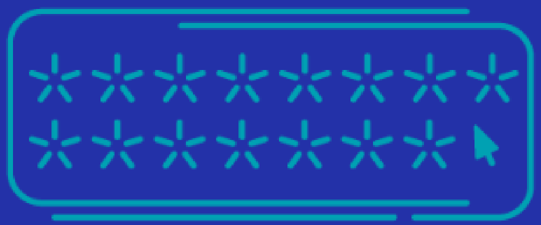
BASICS

Comprendre les concepts de sécurité numérique de base, et savoir où aller pour trouver plus d'aide, est un première étape pour toutes celles et ceux qui travaillent en bibliothèque. Ces compétences n'aident pas seulement à rendre la bibliothèque et ses données plus sécurisées, elles aident également le personnel à mieux aider les usagers à être plus en sécurité en ligne. Ce guide s'adresse aux personnes qui souhaitent acquérir des compétences en matière de sécurité numérique.

Créer des mots de passe robustes

Fermez-vous la porte de chez vous en partant ? La plupart d’entre nous répondons probablement oui à cette question. Pourquoi verrouillons-nous notre porte ? Nous fermons nos maisons parce que nous avons des choses à l’intérieur que nous voulons protéger. Créer un mot de passe robuste est comme avoir une clé unique qui verrouille votre maison. Nous devons avoir la garantie que le verrou est robuste.

Les mots de passe sont dépassés, vive les phrases de passe



Se souvenir de mots de passe pour des dizaines de comptes est un véritable défi. Avoir un mot de passe unique pour chaque compte en ligne devient vite ingérable. Comment peut faire un humain pour réussir pour avoir un mot de passe robuste unique et s'en souvenir ? Grâce aux phrases de passes !

ASTUCE

Oubliez le remplacement des « i » par des 1, des « A » par des « 4 » et des « E » par des « 3 ». Ces techniques sont répandues et connues des pirates. Les logiciels conçus pour cracker des mots de passes testent ces combinaisons

EXERCICE

Entraînez-vous à créer des phrases de passe. Les recommandations actuelles en matière de sécurité préconisent au moins 17 caractères, espaces compris.

- Imaginez une série de mots qui font sens pour vous et que vous pourrez retenir. Cela ne doit contenir aucune information personnelles comme une date de naissance, une adresse ou un nom. Combinez un ensemble de mots pour créer une phrase aléatoire.
- Ajoutez des chiffres et des symboles au début, au milieu ou à la fin de la phrase.
- Maintenant, testez votre phrase de passe sur le site https://www.security.org/how-secure-is-my-password/ et observez en combien de temps votre mot de passe peut être cassé.

Gestionnaires de mots de passe

Combien de mots de passe êtes-vous amenés à retenir au travail ? Les avez-vous écrits sur un post-it soigneusement caché sous votre clavier ou dans un tiroir de votre bureau ? Un des moyens pour se prémunir d'un vol de mots de passe ou de le laisser à la vue de tous est d'utiliser un gestionnaire de mots de passe.

Les gestionnaires de mots de passe génèrent et stockent des mots de passe complexes. Il suffit juste de se souvenir du mot de passe principal (unique et robuste) pour accéder et utiliser le gestionnaire de mots de passe. De plus, les administrations ou les entreprises peuvent acheter des gestionnaires de mots de passes d'équipe pour gérer des comptes partagés.

- Explorez les gestionnaires de mots de passe indiqués, créez-vous un compte et testez.
- Utilisez votre phrase de passe la plus forte comme mot de passe de votre gestionnaire

ESSAYEZ UN GESTIONNAIRE DE MOTS DE PASSE

Dashlane
https://www.dashlane.com/fr

1Password
https://1password.com/fr

LastPass
https://www.lastpass.com/fr

ASTUCE

Sauvegardez-vous vos mots de passe dans votre navigateur ? Attention ! Ce n'est pas sécurisé et des failles de sécurité des navigateurs peuvent permettre à des pirates d'accéder aux mots de passe. Les gestionnaires de mots de passe rendent cette tâche plus complexe.

L'authentification multi-facteurs

Ajoutez un verrou à vos portes numériques

WHO IS THIS IS?

Pour les comptes qui contiennent beaucoup de données personnelles, nous voulons être certains que nous sommes les seuls à pouvoir y accéder. L'authentification multi-facteurs (MFA) signifie que la saisie d'un seul mot de passe n'est pas suffisante pour un pirate qui tente d'accéder à un votre compte. L'authentification à double facteurs (2FA), qui est une déclinaison du MFA, requiert l'ajout d'un code supplémentaire pour autoriser l'accès à votre compte.

Avec le MFA, quand vous saisissez votre mot de passe pour accéder à un service en ligne, vous êtes invités à vérifier votre identité d'une autre façon. La plupart du temps, vous recevez un code par SMS. Ce code à usage unique est nécessaire pour finaliser l'authentification à votre compte. Parfois, la MFA utilise une application tierce, un objet physique (YubiKey ou une information biométrique (empreinte digitale, visage).

Si vous recevez un code par SMS sans que vous ayez tenté de vous connecter à un compte, cela signifie que quelqu'un d'autre tente d'accéder à vote place. C'est le bon moment pour changer votre mot de passe.

EXERCICE

- Passez en revue les comptes que vous détenez en ligne et activez la double authentification si le service le propose.

SERVICE	MFA (Oui / Non)

- L'authentification multi-facteurs peut également être utilisée en bibliothèque. A quels services cette fonctionnalité pourrait-elle être appliquée ?

Hameçonnage

La plupart des bibliothèques utilisent des filtres anti-spam mais cela ne signifie pas que vous n'êtes pas à l'abri de recevoir un mail malveillant

ÉVITEZ DE VOUS FAIRE ATTRAPER

- Cliquez uniquement sur les liens dont vous connaissez la source
- Ne téléchargez pas de pièce-jointe si vous ne connaissez pas l'expéditeur
- Ne communiquez pas d'informations personnelles (carte bancaire, mot de passe…)
- Repérez les indices qui montrent que c'est une arnaque. Ce n'est pas parce qu'un email ressemble à celui qu'un collègue pourrait vous envoyer qu'il s'agit d'un mail légitime. Un pirate peut envoyer un message qui semble être envoyé par un collègue en piratant sa boîte mails ou en recourant aux méthodes d'emails spoofing (du spam par usurpation d'adresse ip)
- Vérifiez l'url sur laquelle on vous demande de cliquer. Est-ce la même adresse que celle du site que vous tapez habituellement ?

ASTUCE

Si vous avez cliqué sur un lien qui vous semble malveillant, signalez-le à votre service informatique

Malware = Logiciel malveillant

Les malwares sont des logiciels conçus pour endommager ou réaliser des actions non désirées sur votre ordinateur ou votre smartphone. En général, ce genre de logiciels s'installe sur votre appareil quand vous téléchargez une pièce-jointe ou cliquez sur un lien ou une publicité. Il peut aussi s'installer si quelqu'un insère un support de stockage externe sur votre machine. Si vous recevez un mail et que vous ne savez pas ce que contient le fichier joint, ne le téléchargez pas !

ASTUCE

Vérifiez si votre adresse mail a déjà fait l'objet d'une fuite suite à un piratage
https://haveibeenpwned.com/

CHECK-LIST POUR SECURISER SON ESPACE DE TRAVAIL

- Vérifiez si vos ordinateurs disposent d'antivirus. Est-ce que les ordinateurs pour le public ont le même niveau de protection que les ordinateurs du personnel ? Est-ce que les ordinateurs public sont sur le même domaine que ceux du personnel ?
- Vérifiez si les dernières mises à jour sont installées sur vos appareils
- Créer un calendrier pour vérifier régulièrement les mises à jour du système d'exploitation et des logiciels quand des nouvelles versions sont publiées afin de corriger des failles et des vulnérabilités qui sont exploitées par des malwares. Cela inclut les ordinateurs et tous les équipements mobiles !
- Est-ce que votre bibliothèque autorise l'utilisation de support de stockage externe ? Créez des procédures qui n'autorisent pas le personnel à brancher des périphériques de stockage externes des usagers sur les appareils du personnel.

Ransomware

Une des catégories de malware qui gagne en popularité est le ransomware. Comment cela fonctionne-t-il ?

En téléchargeant accidentellement un malware, l'assaillant obtient un accès à votre ordinateur, et ensuite il garde en otage vos données stockées sur l'appareil. Le pirate peut verrouiller l'ensemble de vos fichiers ou vous déconnecter de votre réseau et vous demande de payer une rançon pour récupérer l'accès à vos données. Si les fichiers sont importants pour vous, assurez-vous de réaliser des sauvegardes sur des disques externe ou sur un cloud.

ASTUCE

Mettez à jour régulièrement vos appareils. Les mises à jour sont des patchs de sécurité. Vos données et logiciels ne sont protégés que si vous utilisez les dernières versions.

EXERCICE

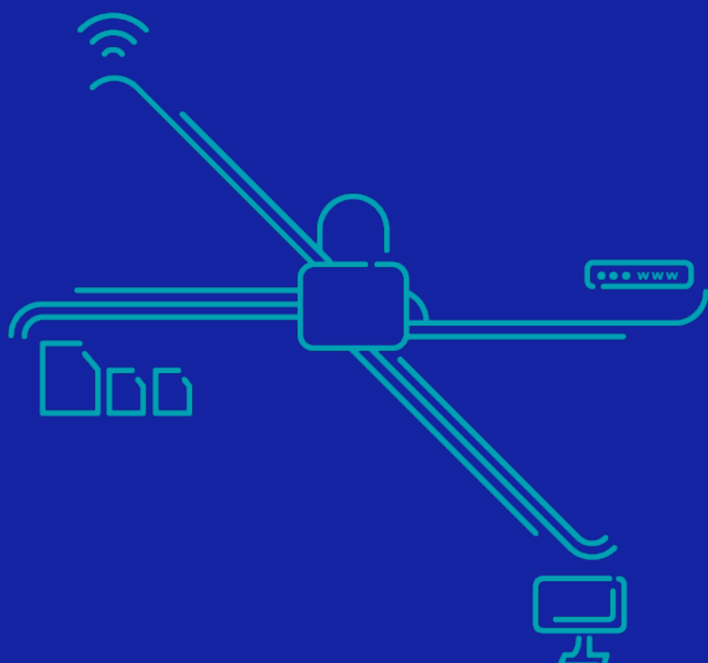
- Effectuez une recherche sur les attaques par ransomware dans les bibliothèques. Combien d'établissements avez-vous pu identifier ?

  ____

  ____

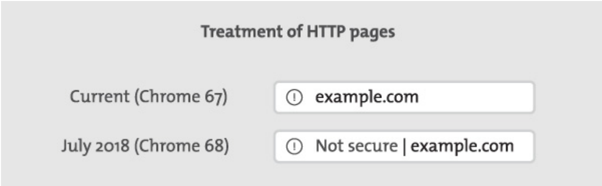
- Est-ce que votre bibliothèque a une procédure en cas d'attaque de ransomware ? Prenez contact auprès de votre service informatique et vos prestataires et posez-leur la question. Si aucun plan n'existe, essayez d'en développer un :
  - Comment le personnel peut-il être contacté sans mail ?
  - Comment les usagers seront-ils notifiés ?
  - La bibliothèque dispose-t-elle d'une méthode pour vérifier les documents sans SIGB ?

Confidentialité du réseau



Consultez le site web de votre bibliothèque. Regardez la barre d'adresse. Voyez-vous un cadenas ouvert ou fermé ? Est-ce que votre adresse indique http ou https ? Le « S » à la fin de https est synonyme de sécurité. Cela signifie que l'ensemble des communication entre votre navigateur et le serveur qui héberge le site sont chiffrées. Ainsi, personne ne peut lire les données qui sont échangées.

C'est vraiment important que le site de votre bibliothèque utilise HTTPS, en particulier pour accéder au compte de l'utilisateur. Par ailleurs, les personnes qui visitent votre site sans HTTPS pourraient recevoir un avertissement de leur navigateur indiquant que le site qu'ils visitent n'est pas sécurisé.



OBTENIR UN ACCÈS HTTPS

- Demandez à votre service informatique d'acheter un certificat TLS. Il existe également des certificats de sécurité gratuits avec Let's Encrypts https://letsencrypt.org/fr/getting-started/ qui permet de générer des certificats pour tous les titulaires de nom de domaine. Une large communauté existe pour vous accompagner dans l'installation du certificat pour obtenir un site web sécurisé.

EXERCICE

- Consultez le site de votre bibliothèque
- Si votre site est encore accessible qu'en HTTP, contactez votre service informatique ou votre prestataire
- SI votre site est sécurisé, visitez quelques sites de bibliothèques conçus par votre prestataire pour vérifier si les sites sont sécurisés.

Formation du personnel et des usagers

Maintenant que vous avez compris les bases, il est temps de partager vos connaissances dans votre établissement. Quand on parle de formation du personnel, il faut penser à :

- comment obtenir l'adhésion du personnel ? Expliquez les enjeux de la protection de la vie privée et pourquoi c'est indispensable dans le fonctionnement de la bibliothèques.
- les compétences techniques du personnel, commencez avec les bases. Ce guide est conçu pour aider tous les agents, y compris ceux qui sont moins à l'aise avec la technologie.
- aux pistes d'améliorations pour continuer à former le personnel.

Même une courte session avec les sujets abordés dans ce guide suffit à renforcer la sécurité de la bibliothèque pour le personnel et les usagers. Utilisez ces cours et ces activités pour organiser des sessions de formations en interne. Vous pouvez aussi utilisez les ressources disponibles en ligne.

Détective de la sécurité numérique

Vous maîtrisez désormais les bases en matière de sécurité numérique. Mettez en pratique vos nouvelles compétences en lisant ces témoignages d'agents sur le terrain.

RENCONTRE AVEC JAMIE

Jamie travaille dans les services techniques d'une bibliothèque et effectue quelques heures de service public. Elle arrive au travail et se connecte à son ordinateur, au SIGB et une application de messagerie pour échanger avec ses collègues, et à l'intranet. Elle utilise un seul mot de passe pour tout ces comptes. Cependant, le service informatique a rappelé qu'il fallait utiliser un mot de passe complexe et unique pour chaque service. C'est trop difficile de se souvenir de chaque alors Jamie a écrit ses mots de passes sur un post-it qu'elle range dans le tiroir de son bureau.

Quand elle est à une banque d'accueil, elle doit se connecter à chaque service et penser à se déconnecter à la fin de sa plage de service public car elle utilise un ordinateur partagé. Parfois, Jamie apporte sa liste de mots de passe qu'elle range dans un tiroir de la banque d'accueil qui n'est pas fermé à clé. A la fin de chaque service, elle rapporte sa liste de mots de passe à l'exception de quelques fois où elle l'a oubliée et récupérée le lendemain matin.

Quelles recommandations feriez-vous à Jamie pour renforcer ses règles d'hygiène numérique ?

RENCONTRE AVEC MEL

Mel travaille en section adulte dans une bibliothèque très fréquentée. Hier, un usager est venue la voir au bureau d'accueil pour lui expliquer qu'il avait un problème avec un ordinateur de la bibliothèque. Il lui a expliqué qu'il souhaitait imprimer un document très important mais qu'il n'y parvenait pas depuis les ordinateurs de la bibliothèque. Mel accompagne l'usager aux ordinateurs et constate qu'ils sont tous occupés. Mel est embarrassée et commence à paniquer. L'usager lui explique qu'il est en retard pour un entretien d'embauche et qu'il a vraiment besoin d'apporter ce document avec lui sinon il ne sera pas recruté. Il explique à Mel qu'il a une clé USB et lui demande si elle peut imprimer son document depuis l'ordinateur du personnel.

Mel, qui souhaite aider l'usager à obtenir son poste, accepte. Elle branche la clé USB, ouvre le document, l'imprime et rend la clé à l'usager. Ce dernier semble excessivement reconnaissant et quitte la bibliothèque précipitamment.

Quand Mel arrive au travaille le lendemain tous les ordinateurs sont déconnectés et elle voit le personnel de la DSI s'agiter frénétiquement. Un responsable lui explique que la bibliothèque a été victime d'un ransomware. L'ensemble des ordinateurs sont paralysés et le pirate demande de payer une rançon en Bitcoin pour récupérer un accès aux ordinateurs.

Quelle erreur en matière de cybersécurité a été commise ?

GUIDE DE DÉFENSE DE LA VIE PRIVEE

La protection de la vie privée est une valeur fondamentale des bibliothèques mais elle est souvent perçue comme une activité difficile et onéreuse. Utilisez ces guides pour commencer à aborder la question de la protection de la vie privée dans votre bibliothèque. Chaque guide propose des exercices pratiques pour les bibliothèques. Consultez ces guides à l'adresse **https://libraryprivacyguides.org/**

This project was made possible in part by the Institute of Museum and Library Services LG-36-19-0073-19.

Designed by PixelbyInch.com