SÉCURITÉ NUMÉRIQUE : MOT DE PASSE

Atelier créé par Yusuf Ganyana (twitter.com/flesymz) pour DiGITAL YOU 2022 (#DigitalYou)

Temps : env. 120 minutes

Question essentielle

Quelle différence cela ferait-il si vous passiez d'un mot de passe facile à deviner à un mot de passe sécurisé ?

Objectif établi

Les participants à cette session apprendront l'importance de protéger leurs appareils et leurs données à mesure que l'utilisation des systèmes informatiques et d'Internet se développe.

Objectifs:

À la fin de la leçon, les participants seront en mesure de :

- Avoir une compréhension de base de la sécurité numérique
- Découvrez pourquoi des mots de passe forts sont nécessaires.
- Recueillir des conseils pour protéger en toute sécurité leur appareil numérique et leurs données.

Matériel de session de formation :

- Projecteur et diapositives de présentation
- Documents de présentation au cas où il n'y aurait pas de projecteur
- Copies du programme de l'atelier
- Copies des documents et des instructions pour les activités
- Papeterie : affiches, marqueurs, stylos, blocs-notes, notes autocollantes
- Copie de la feuille de présence
- Copies du formulaire de consentement photo

APERÇU DE LA MATIERE

Un mot de passe est votre première ligne de défense contre l'accès non autorisé à votre ordinateur et à vos informations personnelles ; chaque jour, plus de sept millions de violations de données se produisent. Si vous utilisez un mot de passe sécurisé, vous êtes moins susceptible d'être attaqué par des pirates et des logiciels malveillants.
Malgré les progrès technologiques exponentiels et la dépendance à l'égard des ordinateurs et d'Internet, l'erreur humaine continue d'être le maillon le plus faible de cette entreprise, car les pirates développent de nouvelles tactiques pour violer les systèmes et les comptes.
Cet atelier sensibilisera à la manière de rester en sécurité dans le monde numérique.

Cet atelier a été inspiré par le kit Digital Enquirer de Tactical Tech.

Type d'atelier : Hors ligne

- Copies du formulaire d'évaluation/d'enquête

NOTES D'ANIMATION

PRÉSENTATION - 10 minutes

- L'hôte explique les règles d'entretien telles que :
  - Emplacement des salles de bain
  - Utilisation des téléphones portables
  - Consentement photo,
  - Signer la feuille de présence
  - Partagez le programme de l'atelier
- Hôte pour accueillir le(s) facilitateur(s)
- Le ou les animateurs se sont présentés, ont donné un bref aperçu de l'atelier, c'est-à-dire le titre, les objectifs et les résultats attendus.
- Les animateurs doivent solliciter les attentes des participants et ajuster la leçon en conséquence.
- Facilitateur(s) pour donner un bref aperçu de Tactical Tech et du GOETHE INSTITUT.

BRISE -GLACE - 5 minutes

CHARADE DE MOT DE PASSE

[INVITEZ] Les participants à écrire un mot de passe facile à deviner sur une note autocollante, mais pas leurs mots de passe réels.

- Ramassez les notes autocollantes et disposez-les sur une table, face vers le bas.
- À l'aide du formulaire de présence signé, sélectionnez un participant au hasard et demandez-lui de "jouer" un mot de passe sans parler.
- **[ENCOURAGEZ]** les autres participants à deviner de quoi il s'agit.
- **[RAPPELEZ-** leur] de continuer jusqu'à la fin des cinq minutes.

SÉCURITÉ NUMÉRIQUE : MOT DE PASSE

Atelier créé par Yusuf Ganyana (twitter.com/flesymz) pour DiGITAL YOU 2022 (#DigitalYou)

– LEÇON PRINCIPALE –

60-90 minutes

[DEMANDER] ***Qu'est-ce que nous essayons de protéger ?***

Remarque *: Racontez une histoire à laquelle ils peuvent s'identifier.*

EXPLAIN

Je ne sais pas comment vous vous sentiriez si vous égariez votre téléphone. Je vivrais littéralement une mini-crise cardiaque, démontrant à quel point les appareils numériques sont devenus indispensables. Il n'est pas surprenant que nos smartphones nous connaissent mieux que nous nous connaissons nous-mêmes ; par exemple, nos téléphones sont au courant de nos conversations (historique des appels, SMS des amis et de la famille), de nos exploits (photos et historique de localisation), etc. La confidentialité des données que nous générons, ainsi que la vie privée de nos familles et amis doivent être protégées.

[ENCOURAGEZ] les participants à identifier certaines des données sur leurs smartphones.

[RAPPELEZ-VOUS] Faites une pause périodiquement pour vous assurer que le concept est compris

[POSER] ***Qu'est-ce que la sécurité numérique ?***

Exemple de réponse

La protection des informations, des appareils et des comptes contre les accès non autorisés et les attaques malveillantes, permettant aux utilisateurs d'utiliser les médias sociaux, Internet et les services en ligne (tels que les services bancaires numériques) tout en préservant la confidentialité et l'intégrité de leurs données sensibles.

En termes simples, la défense de notre identité numérique ou, en hypothèse, l'autodéfense numérique.

[PAUSE] Des questions ?

[POSER] Pourquoi la sécurité numérique est-elle importante ?

Exemples de réponses

Il permet aux utilisateurs d'utiliser les médias sociaux, Internet et les services en ligne (tels que les services bancaires numériques) tout en protégeant la confidentialité et l'intégrité de leurs données sensibles.

- Pour protéger la **confidentialité** de notre présence en ligne.
- Réduire la possibilité de violations de données ; **intégrité** .
- Accorder aux utilisateurs autorisés l'accès aux informations ; **disponibilité** .

[EMPHASIZE] Pour mettre en œuvre efficacement la sécurité numérique, vous devez apprendre en permanence les nouvelles tendances.

[PAUSE] Des questions ?

[POSER] Comment prioriser une bonne hygiène numérique ?

[EXPLIQUER] L'hygiène numérique est un ensemble de pratiques que vous suivez religieusement afin de sécuriser vos données et vos appareils.

Exemples de réponses

- Sachez que vous êtes une cible pour les cybercriminels.
- Ne prenez jamais de raccourcis, comme réutiliser le même mot de passe.
- Utilisez un code PIN ou un mot de passe pour verrouiller votre appareil et ne le laissez jamais sans protection en public.
- Gardez vos logiciels et votre matériel à jour.
- Installez des applications uniquement à partir de sources fiables.
- Vérifiez les liens avant de cliquer ; n'ouvrez pas de liens ou de pièces jointes dans des e-mails ou des SMS non sollicités.
- Protégez-vous avec un logiciel anti-virus et anti-malware.
- Configurez des mots de passe forts et activez l'authentification à deux facteurs.
- Sauvegardez toujours fréquemment les données importantes.
- Avant d'utiliser des périphériques externes, analysez-les toujours à la recherche de virus.
- Il est conseillé d'utiliser un VPN si vous vous connectez à un réseau public.

[PAUSE] Des questions ?

[DEMANDER] ***Qu'est-ce qu'un mot de passe ?***

Exemple de réponse

Une combinaison de lettres, de chiffres et de caractères spéciaux utilisée pour vérifier l'identité et accorder l'accès tout en empêchant l'accès non autorisé.

Il est également connu sous le nom de signature numérique car il vous identifie de manière unique.

[**ASK**] ***Pourquoi un mot de passe est-il important ?***

Exemple de réponse

Protégez vos données contre tout accès non autorisé, en évitant la perte d'informations précieuses, les violations financières, le vol d'identité et d'autres problèmes.

[PAUSE] Des questions ?

[DEMANDER] ***Qu'est-ce qu'une phrase secrète ?***

Exemples de réponses

Il fonctionne de la même manière qu'un mot de passe, mais il utilise une combinaison de mots communs aléatoires pour créer une signature numérique semblable à une phrase que seul le propriétaire comprend.

[PAUSE] Des questions ?

[DISCUSS] ***Pourquoi est-il recommandé d'utiliser une phrase secrète comme alternative au mot de passe ?***

Exemples de réponses

- Plus long qu'un mot de passe traditionnel pour plus de sécurité.
- Facile à retenir
- Difficile à craquer.

[PAUSE] Des questions ?

Activité

CRÉER UNE PHRASE MOT DE PASSE À L'AIDE D'UN DÉS

[RAPPELEZ-VOUS] Félicitez-les d'avoir terminé cette tâche.

[POSER] ***Qu'est-ce qui rend un mot de passe faible ?***

[INVITEZ] Les participants à se rendre sur ce site Web , à entrer les mots de passe qu'ils ont écrits pendant le brise-glace et à partager leurs réflexions.

Exemple de réponse

1. Utilisation des informations personnelles
2. Utilise des mots et des modèles de clavier courants
3. Utiliser des mots du dictionnaire ; à moins de créer une phrase de passe
4. Réutiliser d'anciens mots de passe ou utiliser le même mot de passe à plusieurs endroits
5. Utilisation des mots de passe par défaut
6. Utiliser un mot de passe de moins de huit caractères
7. Stocker votre mot de passe dans un emplacement facilement accessible, comme une note autocollante ou un fichier non sécurisé sur votre ordinateur.

[EMPHASIZE] Même un mot de passe fort peut être faible s'il n'est pas stocké en toute sécurité. C'est la même chose que de construire un grand coffre-fort en métal pour ranger tous vos objets de valeur, puis de placer la clé directement sur le coffre-fort ; cela ne fournira aucune sécurité.

[PAUSE] Des questions ?

[POSER] ***Pourquoi les gens utilisent-ils des mots de passe faibles ?***

[INVITER] Les participants à délibérer sur ce

Exemple de réponse

- Il peut être difficile de se souvenir de tous les mots de passe des différents services qui en ont besoin.
- Parce que les utilisateurs sont habitués aux raccourcis, les mots de passe sont fréquemment réutilisés.
- Lorsqu'un mot de passe fort n'est pas requis par une stratégie système.

[PAUSE] Des questions ?

[DEMANDER] Quels sont les effets de l'utilisation d'un mot de passe faible.

Exemple de réponse

- Vous devenez une cible pour les pirates.
- Vous pourriez être victime d'un vol d'identité.

- Vos données compromises pourraient être utilisées pour commettre un crime.
- Chantage
- Perte d'intimité

[PAUSE] Des questions ?

[ASK] ***Quelles questions peut-on se poser pour créer un mot de passe plus fort ?***

Exemple de réponse

- La prise en charge des mots de passe est-elle disponible ?
- Est-ce la longueur recommandée ?
- Inclut-il un mélange de caractères?
- Que fait-il pour empêcher les derniers tours des hackers ?
- Est-il unique pour mes autres mots de passe ?
- Des informations personnelles y sont-elles contenues ?
- Est-il assez complexe pour être piraté, mais assez simple pour qu'on s'en souvienne ?
- L'authentification multifacteur peut-elle être utilisée ?

[**ENCOURAGEZ**] les participants à s'abstenir de faire des substitutions évidentes de personnages. Par exemple, les pirates intègrent désormais la lettre "O" au lieu du zéro "0" dans leur code.

[PAUSE] Des questions ?

[ASK] ***Qu'est-ce que l'authentification multifacteur (MFA) ?***

Exemple de réponse
Il s'agit d'un type d'authentification électronique dans lequel un utilisateur n'a accès à un site Web ou à une application qu'après avoir présenté avec succès deux éléments de preuve ou plus à un mécanisme d'authentification.

[PAUSE] Des questions ?

[ASK] ***Pourquoi la MFA est-elle importante ?***

Exemple de réponse

La MFA empêche l'accès non autorisé à vos données personnelles, même si votre mot de passe est compromis, car des informations d'identification compromises ne peuvent pas fournir les facteurs d'authentification supplémentaires requis.

[PAUSE] Des questions ?

[**ASK**] Comment fonctionne MFA ?

Exemple de réponse

Il utilise deux ou trois facteurs d'authentification :

- Quelque chose qui vous est familier, comme votre mot de **passe** .
- Quelque chose que vous possédez, par exemple un code à usage unique envoyé sur votre **smartphone** .
- Quelque chose qui vous est unique, comme vos **empreintes digitales** .

[POSER] Comment pouvez-vous sécuriser votre mot de passe ?

Exemple de réponse

- Soyez toujours à l'affût des tentatives de phishing et ne partagez votre mot de passe avec personne.
- Utilisez un logiciel anti-malware.
- Remplacez votre mot de passe par une phrase secrète.
- Assurez-vous de modifier tout mot de passe généré automatiquement ou par défaut.
- Évitez d'écrire les mots de passe.
- N'utilisez jamais votre mot de passe sur un réseau sans fil public qui n'est pas sécurisé. Si vous pensez que votre mot de passe a été compromis, changez-le immédiatement.
- Évitez de laisser votre ordinateur se souvenir de votre mot de passe.
- Activez l'authentification à deux facteurs.

[DEMANDER] ***Quelles sont les meilleures pratiques pour protéger mon mot de passe lorsque j'utilise un ordinateur public ?***

[POINT OUT] Bien que les ordinateurs publics soient pratiques, ils sont plus susceptibles d'être infectés par des logiciels malveillants.

- Utilisez un programme de détection de logiciels espions en ligne réputé.

- Désactivez la saisie semi-automatique ou la fonction d'enregistrement du mot de passe ; n'enregistrez pas vos informations de connexion.
- Déconnectez-vous toujours avant de fermer la fenêtre du navigateur.
- Effacez votre historique et vos fichiers Internet temporaires en utilisant le mode Incognito.
- Soyez à l'affût des personnes qui regardent votre écran.
- Évitez de saisir des informations sensibles sur un ordinateur public, comme une transaction financière qui pourrait révéler un mot de passe.
- N'utilisez pas votre disque dur externe. Il pourrait choisir des logiciels malveillants.

Questions et réponses

[ASK] ***Quelles questions avez-vous pour moi ?***

[INVITER] et encouragez les participants à poser des questions ou à demander des éclaircissements sur un point qui n'était pas clair ou, dans une certaine mesure, sur des attentes non satisfaites.

-CONCLUSION-

10 minutes

En pratiquant une bonne hygiène numérique, nous pouvons limiter les erreurs les plus courantes que nous commettons et qui conduisent à l'exposition de nos mots de passe à des personnes malveillantes. Cela protégera notre vie privée. Il ne s'agit pas seulement d'assurer le bon fonctionnement de nos appareils ; il s'agit également de nous protéger d'une liste sans cesse croissante de menaces en ligne.

Emballer

[DISTRIBUEZ] le formulaire d'évaluation et laissez-leur le temps de le remplir.

[RAPPELEZ-VOUS] Rassemblez les formulaires avant leur départ.

[REMERCIEZ]-les pour leur participation et **[ENCOURAGEZ** -les] à partager ce qu'ils ont appris avec leur famille et leurs amis.

- FIN