RÉGION ACADÉMIQUE
AUVERGNE-
RHÔNE-ALPES

Liberté
Égalité
Fraternité

Délégation régionale académique
au numérique éducatif

COMPORTEMENT DE PRUDENCE

Phishing, mot de passe robuste, bonnes pratiques

AMBASSADEURS ET AMBASSADRICE PIX AURA

- Clermont - Jean-Philippe Bliek
- Grenoble - Emmanuel Gaunard
- Lyon - Perrine Douhéret

LE PISHING OU HAMMEÇONNAGE

Vidéo phishing

Définition

L'hameçonnage ou phishing en anglais est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux mail, SMS, un message sur les réseaux sociaux ou un appel téléphonique.

Source : Cybermalveillance.gouv

Techniques utilisées :

- Imitation de sites web légitimes
- Utilisation de logiciels malveillants distribués via des liens ou pièces jointes infectées

BONNES PRATIQUES

Précautions :

1. Ne **divulguez jamais d'informations sensibles** par messagerie ou téléphone.
2. Passez la souris sur les liens douteux pour **vérifier l'adresse avant de cliquer.**
3. **Ne pas cliquer sur les pièces jointes**
4. Vérifiez **l'adresse URL des sites**.
5. En cas de doute, **contactez directement** l'organisme concerné.
6. Utilisez **des mots de passe différents et complexes** pour chaque site et application.
7. Activez la **double authentification** pour sécuriser vos accès, si disponible.

Un site pour vérifier les adresses : Phishing initiative	**Signaler :** Signal Spam	**Se faire aider :** Cybermalveillance.gouv.fr

RÉAGIR

Individuellement

- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le

MOT DE PASSE ROBUSTE

Longueur : 12 à 16 caractères
Complexité : Il doit inclure une combinaison des différents types de caractères (aA&1)
Imprévisibilité : Éviter les mots de passe évidents ou des informations personnelles facilement devinables
Passphrases : Utiliser des phrases de mots aléatoires (par exemple, "ChienBleu!Soleil@Lune123") qui sont plus faciles à retenir tout en restant sécurisées.

MOT DE PASSE

- Un service, un site ou une application = un mot de passe unique
- Ne plus jamais réutiliser un mot de passe compromis
- Changer les mots de passe régulièrement
- Favoriser l'authentification multi facteur (« MFA »)
- Utiliser un gestionnaire de mot de passe sécurisé pour stocker vos mots de passe

En cas d'utilisation d'un appareil partagé,

- n'enregistrer pas vos mots de passe
- utiliser une session personnelle sécurisée par un mot de passe robuste
- Se déconnecter de vos applications et de votre session.

VIOLATION DE DONNÉES PERSONNELLES

Une violation de données personnelles est un incident de sécurité portant sur les données dont un établissement à la charge. Cela peut être une divulgation, une altération, une perte des données personnelles.

Elle peut être accidentelle, intentionnelle, malveillante ou non, interne ou externe à l'établissement.

Elle a nécessairement des conséquences sur les personnes concernées par la violation, portant atteinte à la confidentialité, l'intégrité ou la disponibilité de leurs données personnelles.

RSSI : Responsable de la Sécurité des Systèmes d'Information - dsi@ac-lyon.fr
DPD : Délégué à la Protection des Données - dpd@ac-lyon.fr

MES RÉFLEXES

En cas de risque élevé, le DPD doit notifier la CNIL dans un délai de 72 heures.

1. Identifier la violation
2. Dater la violation
3. Alerter le DPD et le RSSI
   securite-donnees@ac-lyon.fr
4. Mettre en place des contre-mesures
5. Évaluer la situation avec le DPD et le RSSI
6. Documenter

ACADÉMIE DE LYON
Liberté
Égalité
Fraternité

IMPACTS

Il suffit d'une seule intrusion dans un système pour entraîner :

- **la perturbation des services**, voire l'arrêt de l'activité du service ;
- **l'inaccessibilité, la destruction, le vol, ou la diffusion des données** des enseignants, des parents, des élèves ;
- **des risques sociaux et psycho-sociaux** pour les personnes exposées ;
- **des risques juridiques** : la responsabilité* (civile, pénale et administrative) du rectorat peut en effet être engagée.

CRCN

DOMAINE 1 : INFORMATIONS ET DONNÉES

1.1 Mener une recherche et une veille d'information
1.2 Gérer des données
1.3Traiter des données

DOMAINE 2 : COMMUNICATION ET COLLABORATION

2.1 Interagir
2.2 Partager et publier
2.3 Collaborer
2.4 S'insérer dans le monde numérique

DOMAINE 3 : CRÉATION DE CONTENUS

3.1 Développer des documents textuels
3.2 Développer des documents multimédias
3.3 Adapter des documents à leur finalité
3.4 Programmer

DOMAINE 4 : PROTECTION ET SÉCURITÉ

4.1 Sécuriser l'environnement numérique
4.2 Protéger les données personnelles et la vie privée
4.3 Protéger la santé, le bien-être et l'environnement

DOMAINE 5 : ENVIRONNEMENT ET NUMÉRIQUE

5.1 Résoudre des problèmes techniques
5.2 Évoluer dans un environnement numérique

CRCN-Édu

DOMAINE 1 : ENGAGEMENT PROFESSIONNEL

1.1 Communiquer
1.2 Collaborer
1.3 Se former, développer une veille
1.4 Agir en faveur d'un numérique sûr et responsable
1.5 Adopter une posture ouverte, critique, réflexive

DOMAINE 2 : RESSOURCES NUMÉRIQUES

2.1 Sélectionner des ressources
2.2 Concevoir des ressources
2.3 Gérer des ressources

DOMAINE 3 : ENSEIGNEMENT - APPRENTISSAGE

3.1 Concevoir
3.2 Mettre en œuvre
3.3 Évaluer au service des apprentissages

DOMAINE 4 : DIVERSITÉ ET AUTONOMIE DES APPRENANTS

4.1 Inclure et rendre accessible
4.2 Différencier
4.3 Engager les apprenants

DOMAINE 5 : COMPÉTENCES NUMÉRIQUES DES APPRENANTS

5.1 Développer les compétences numériques des apprenants
5.2 Évaluer et certifier

PIX+ÉDU NUMÉRIQUE ET SÉCURITÉ

Pour aller plus loin et approfondir vos compétences, nous vous conseillons de réaliser **le parcours Pix+Edu thématique "Numérique et sécurité"**, qui couvre les questions abordées aujourd'hui.

- **Durée moyenne :** Entre 1 et 2 heures
- **Format :** Environ 40 questions et défis formatifs, adaptés à votre profil et à vos réponses.
- **Flexibilité :** Vous pouvez avancer à votre rythme, suspendre et reprendre le parcours à tout moment.
- **Suivi et accompagnement :** La plateforme Pix permet de visualiser votre progression, ainsi que les réponses et explications associées. Des tutoriels sont également disponibles tout au long du parcours.

SEMAINE PROCHAINE

EXCEPTION PÉDAGOGIQUE

- Reproduction d'œuvres protégées,
- Droits d'auteur

Merci encore

ET À BIENTÔT !

N'hésitez pas à nous contacter pour toute question ou besoin d'assistance supplémentaire.