

Phishing bien ficelé

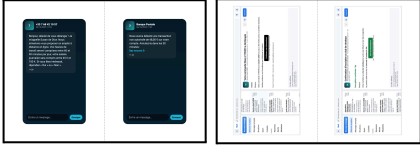
FRÉQUENCE
ÉCOLES

— Guide d'animation


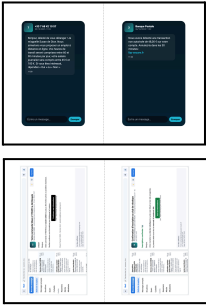
Dans cette activité, les participants analysent des exemples de sites web, de messages et de mails pour déterminer lesquels sont des tentatives de phishing. Ils doivent, pour chaque exemple, identifier les indices qui permettent de savoir si le message ou le mail est de confiance.


Situation	Durée
Enzo a effectué une commande en ligne, et a reçu un SMS de colissimo qui lui demande de payer des frais de livraison. Il se méfie, et se demande si c'est une tentative de phishing.	30 min
Objectif pédagogique	
Reconnaître si un mail ou un SMS est une tentative de phishing	
Prérequis pour les participants	
Savoir ce qu'est un nom de domaine Savoir ce qu'est une tentative de phishing	

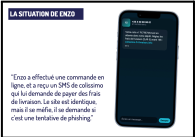
Matériel

Matériel	
1 fiche "situation de Enzo" par groupe	
20 "exemples de message" par groupes	

Déroulé de l'activité

Étape	Temps	Actions des participants	Matériel
Introduction / situation	5 min	<p>Le médiateur ou la médiatrice se présente et accueille le groupe. Il pose le cadre de l'intervention. Il explique le programme de la séance et invite à la participation et à la bienveillance de chacun.</p> <p>Le médiateur ou la médiatrice distribue à chaque groupe une fiche "Situation de Enzo". Il ou elle lit la situation, et pose des questions aux participants pour essayer de créer du lien entre la situation et leurs expériences personnelles. <i>"Est-ce que cette situation vous fait penser à quelque chose que vous avez vécu ? Est-ce que vous recevez parfois des messages suspects ?"</i></p> <p>Le médiateur ou la médiatrice explique : <i>"Pour essayer de mieux comprendre cette situation, nous allons faire une activité, dans laquelle VOUS allez devoir déterminer si ces messages sont des tentatives de phishing (hameçonnage en français) ou non"</i></p>	 Fiches situation
Consignes de l'activité	5min	<p>Le médiateur ou la médiatrice forme des groupes de 4 personnes. Chaque groupe a un exemplaire des fiches "exemples de message".</p> <p>Les participants doivent analyser chacun des exemples, et déterminer, si pour eux, il s'agit d'une tentative d'escroquerie, expliquer pourquoi et se mettre d'accord en groupe. Ils doivent donc les classer en deux catégories : "Message sûr" et "Tentative d'escroquerie".</p>	 Exemples de messages

Étape	Temps	Actions des participants	Matériel
Analyse des exemples	20min	<p>Les participants analysent les différents exemples. Ils doivent notamment faire attention :</p> <ul style="list-style-type: none"> - aux expéditeurs - aux liens contenus - aux noms de domaine utilisés - au levier utilisé (comme l'urgence) <p>Solutions :</p> <ol style="list-style-type: none"> 1. Arnaque : "etudiant-crous.fr-paiement.net" imite le nom de domaine du crous. Ici, le domaine est "fr-paiement.net"; et "etudiant-crous" est le sous-domaine. "À confirmer avant minuit" cherche à créer l'urgence pour faire baisser la vigilance. 2. Arnaque : "C'est qui ?" venant d'un numéro inconnu, que nous n'avons pas appelé ou contacté par message, a de très fortes chances d'être une arnaque. Cette arnaque se répand beaucoup et permet plusieurs choses : valider qu'un numéro est toujours actif si la personne répond, et aussi amener progressivement vers une arnaque dans laquelle on se méfie moins, parce qu'on a l'impression de parler à un humain. 3. Arnaque : "lbp-secure.fr" imite le domaine de la banque postale. "Annulez-la dans les 30 minutes" cherche à créer un sentiment d'urgence pour faire baisser la vigilance de la victime. 4. Arnaque : Arnaque de plus en plus répandue, se faire passer par un proche (et souvent chercher à rediriger la conversation sur un numéro whatsapp) pour demander des fonds "en urgence". 5. Sûr 6. Sûr 7. Arnaque : Arnaque typique de promesse de travail par SMS ; il peut être envoyé à de nombreux utilisateurs, leur demandant ensuite d'effectuer des tâches, et de divulguer des identifiants bancaires pour être payé 8. Sûr 9. Sûr 10. Sûr 11. Arnaque : "vie-scolaire.educ-contact.fr" imite une adresse institutionnelle. Le domaine "educ-contact.fr" est trompeur. "avant 18h sous peine" cherche à créer à l'urgence pour faire baisser la vigilance. 12. Arnaque : "colissimo.fr-livraison.info" imite le domaine de colissimo. Ce n'est pas parce que colissimo est dans l'adresse qu'il s'agit du site légitime. Ici le domaine est "fr-livraison.info". "Avant 18h" cherche à créer l'urgence. "2,49€" est une petite somme, faite pour que l'utilisateur n'hésite pas à rentrer ses identifiants bancaires. 13. Arnaque : Cette arnaque utilise un stratagème subtil mais redoutable : dans l'adresse "rnicrosoft.com" les caractères "r" et "n" sont utilisés pour former un "m" ($r+n = rn = m$). De nombreuses arnaques utilisent cette mécanique, par exemple en utilisant des caractères proches ($i = \dot{i} = \ddot{i}$). 14. Sûr 15. Arnaque : "fnac.offre-bonus.fr" cherche à imiter le domaine de la Fnac. Le cadeau d'un bon d'achat vise à faire baisser la vigilance de la victime. 16. Arnaque : "epicgames-bonus.com" imite Le domaine d'Epic Games. Ce mail utilise l'appât d'une récompense gratuite pour faire baisser la vigilance de l'utilisateur. 	 <p>Exemples de messages</p>

Étape	Temps	Actions des participants	Matériel
		17. Sûr 18. Arnaque : " ent-lyon.fr-securite.net " cherche clairement à imiter l'adresse d'un ENT. La "suspension sous 24h" vise à faire baisser la vigilance de la victime. Ici le sous-domaine est "ent-lyon" et le nom de domaine " fr-securite.net ". Il s'agit d'une technique pour imiter un nom de domaine. 19. Arnaque : " Sheen-shopping.com ", cherche clairement à imiter le nom de la marque de base. 20. Sûr	
Mise en commun	5 min	Les participants mettent en commun leurs avis sur les messages, et partagent les raisons pour lesquelles ils pensent que c'est une tentative d'escroquerie ou non.	
Débrief / conclusion	10 min	<p><i>"Pour conclure cette activité, nous allons revenir à la situation de Enzo. Qu'est-ce que vous en pensez ? Est-ce qu'il doit payer ces frais de livraison ?"</i></p> <p>Qu'ils s'adressent à un élève, à un parent ou à un adulte, les messages de phishing utilisent tous les mêmes leviers psychologiques. Ils exploitent souvent l'urgence, la peur, ou la curiosité pour pousser la victime à agir vite, avant même d'avoir pris le temps de réfléchir.</p> <p>Un lien raccourci ou un nom de domaine trompeur, un ton pressant (« sous 24h », « avant minuit », « dernière chance »), ou encore un message qui semble venir d'une autorité (banque, établissement scolaire, administration...) sont autant d'indices qui doivent alerter.</p> <p>Les cybercriminels jouent sur nos émotions pour détourner notre vigilance. Ils savent que face à un message qui semble officiel ou urgent, nous avons tendance à réagir sans vérifier. C'est cette impulsion qu'ils exploitent pour nous pousser à cliquer sur un lien, à renseigner nos identifiants, ou à effectuer un paiement.</p> <p>Ouverture et questionnements supplémentaires :</p> <ul style="list-style-type: none"> - Quels sont les éléments qui vous ont semblé suspects dans les exemples analysés ? (adresse de l'expéditeur, ton du message, lien douteux, fautes d'orthographe, etc.) - Quels sont au contraire les indices qui rendaient certains messages crédibles ? (mise en page professionnelle, logos, ton institutionnel...) - Pourquoi ces messages visent-ils particulièrement les jeunes ? (habitudes de messagerie, confiance dans les plateformes, manque d'expérience face aux arnaques...) - Quels réflexes adopter avant de cliquer sur un lien reçu par mail ou SMS ? (vérifier le domaine du site, ne pas renseigner ses identifiants, passer par le site officiel, demander confirmation à un adulte ou à l'émetteur supposé) - Connaissez-vous d'autres formes d'arnaques qui cherchent à vous voler des données personnelles ? → Il existe notamment les arnaques par téléphone, où par exemple la personne se fait passer pour votre banque, et vous demande vos identifiants de connexion, ou d'effectuer un virement. Il faut être particulièrement vigilant face à ces appels. Ne donnez JAMAIS d'identifiant par téléphone. En cas de doute, raccrochez, et rappelez vous-même via le numéro officiel qui vous est fourni (via votre application par exemple). 	 <p>Fiches situation</p>