MODULE 5 :
Protection de la vie privée numérique

CONTENU 1 : Comment identifier les contenus dangereux

Ce projet a été financé avec le soutien de la Commission européenne. Cette publication reflète uniquement le point de vue de l'auteur et la Commission n'est pas responsable de l'usage qui pourrait être fait des informations qu'elle contient. 2022-1-TR01-KA220-VET-000088431

Co-funded by the European Union

Contenus dangereux : l'hameçonnage

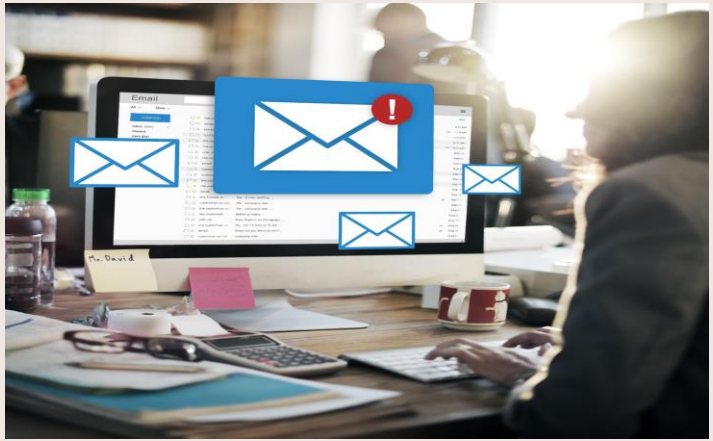
L'hameçonnage, ou phishing est une forme d'escroquerie en ligne qui vise à inciter les utilisateurs à visiter un site Web susceptible d'installer un logiciel malveillant capable de voler des informations sensibles telles que des coordonnées bancaires ou des données personnelles. Le phishing peut être réalisé de plusieurs manières.

Source : freepik

Co-funded by the European Union

Courriers indésirables

Les courriers indésirables non sollicités, également appelés spams, sont envoyés à un large éventail de destinataires sans leur consentement. Bien qu'ils soient généralement envoyés à des fins commerciales, ils peuvent dans certains cas être malveillants.



Source : freepik

Co-funded by the European Union

Comment détecter les spams ?

Nom de l'expéditeur: Un nom généré aléatoirement indique très probablement que le courrier n'est pas légitime, par exemple, john3423.

Erreurs d'orthographe et de grammaire : Les spammeurs sont plus susceptibles de faire des fautes d'orthographe et de grammaire dans leurs courriers, par exemple, « envoyer depui mon appareil ».

Source : freepik

Co-funded by the European Union

Comment détecter les spams ?

Urgence: Les institutions professionnelles, comme votre banque, ne vous demanderont pas d'accomplir une tâche dans un délai excessivement court. La présence d'une contrainte de temps, généralement quelques heures, dans un courriel demandant votre attention immédiate est souvent un signe clair de spam.

Source : freepik

Liens suspects: Lorsqu'une organisation, comme votre banque, vous demande de vous connecter à votre compte dans un but précis, il est conseillé d'aborder les liens qui prétendent mener à leur page de connexion avec scepticisme.

Co-funded by the European Union

Messages textes

Les fraudeurs utilisent des messages textes trompeurs pour tromper les individus et leur demander d'obtenir leurs informations personnelles, telles que des **mots de passe**. La plupart de ces messages incluent souvent des offres de prix gratuits et vous invitent à cliquer sur des liens. Ces messages sont relativement plus faciles à éviter.

Source : freepik

Co-funded by the European Union

EXERCICE

Imaginons que vous informiez quelqu'un qui n'est pas au courant des dangers associés à ces contenus dangereux. Comment décririez-vous chacun d'eux en une seule phrase ? Assurez-vous que votre explication soit courte et percutante.

- L'hameçonnage c'est...
- Le courrier indésirable est ....
- Un message texte trompeur est...

Source : freepik

Co-funded by the European Union

Liens utiles

- Cybercriminalité #1 - Qu’est-ce que le phishing ? - YouTube
- https://cyber.gouv.fr/de-quoi-parle-t-on
- https://cyber.gouv.fr/le-mooc-secnumacademie
- Arnaques : attention aux mails ou aux SMS frauduleux | franceinfo (radiofrance.fr)

- Qu'est-ce que le phishing ? (anglais)
- Qu'est-ce que le smishing ? Comment fonctionne le phishing par SMS (anglais)

Références

- https://www.freepik.com/
- https://shorturl.at/GCB1I
- https://shorturl.at/nDwhZ