

SCRIPT VIDÉO « CACTUS 2026-PERSONNELS ADMINISTRATIF ET ENSEIGNANTS »

« Bonjour,

Si vous regardez cette vidéo, c'est que vous étiez prêt à communiquer des informations personnelles pour des ressources pédagogiques gratuites.

Vous l'aurez compris, il s'agit d'un exercice de sensibilisation à la cybersécurité. Les données que vous étiez prêt à communiquer auraient pu être récupérées et exploitées par un cybercriminel.

Cela s'appelle de l'hameçonnage ou *phishing* en anglais : il s'agit d'un SMS ou d'un email frauduleux envoyé dans le cadre personnel ou professionnel par les cybercriminels. Il est destiné à vous tromper pour vous inciter à communiquer des données personnelles pour les revendre ou les utiliser par la suite. Par exemple pour usurper votre identité.

C'est la menace principale pour le grand public. Aujourd'hui, de nombreuses fuites de données du quotidien nourrissent ce phénomène.

Voici quelques conseils simples qui peuvent vous éviter bien des ennuis.

1. Vérifiez l'expéditeur du message et le langage employé (caractère d'urgence, émotions, bonnes affaires)
2. Vérifiez les liens dans l'email avant de cliquer dessus, dans le but d'identifier si le site est légitime ou non
3. Ne communiquez jamais d'information sensible suite à un message ou un appel
4. Au moindre doute, contactez directement l'organisme concerné pour confirmer
5. N'hésitez pas à contacter l'expéditeur (si il est connu), via un canal autre que celui d'origine; une adresse de messagerie peut aussi être falsifiée
6. Enfin, activez la double authentification lorsque cela est possible

Et si jamais vous êtes victime d'une cybermalveillance, qu'il s'agisse d'un hameçonnage, d'un piratage de compte ou d'un virus, rendez-vous sur 17Cyber.gouv.fr pour trouver de l'assistance.

Merci d'avoir participé à cet exercice de sensibilisation à la cybersécurité.

Vous êtes un acteur essentiel de la chaîne de sécurité de la communauté éducative.

Je vous invite à poursuivre les actions de prévention et de sensibilisation tout au long de l'année. N'hésitez pas à partager ces conseils avec les élèves, vos collègues, vos proches pour utiliser le numérique en toute sécurité.»