SCRIPT VIDÉO « CACTUS 2026-LYCÉENS »

« Bonjour à toutes et à tous.
Si vous regardez cette vidéo, c'est que vous étiez prêt à communiquer des informations personnelles pour accéder à une nouvelle plateforme d'orientation. Vous l'aurez compris, il n'y a pas de service miracle permettant de garantir une place dans l'établissement de son choix sur simple demande…Mais la bonne nouvelle, c'est qu'il s'agit d'un exercice de sensibilisation à la cybersécurité et que les données que vous étiez prêt à communiquer ne seront pas récupérées par un cybercriminel.

Cela s'appelle de l'hameçonnage ou phishing en anglais. Il s'agit d'un SMS ou d'un mail frauduleux envoyé par les cybercriminels et destiné à vous tromper pour vous inciter à communiquer des données personnelles pour les revendre et les réutiliser par la suite, par exemple pour usurper votre identité.

Pour s'en prémunir 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 (s'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. N'hésitez pas à partager ces conseils à vos amis et à votre famille pour utiliser le numérique en toute sécurité. »