SCRIPT VIDÉO « CACTUS 2026-PARENTS D'ÉLEVES »

« Bonjour
Si vous regardez cette vidéo, c'est sans doute que vous avez reçu un message concernant un club de sport ou du matériel gratuit pour vos enfants. Cela s'appelle de l'hameçonnage ou phishing en anglais. Il s'agit d'un SMS ou d'un email frauduleux envoyé par les cybercriminels. Ceci est destiné à vous tromper afin de vous inciter à communiquer des données personnelles pour usurper votre identité par exemple.

Ce message faisait partie d'une campagne nationale de sensibilisation menée dans le cadre de l'éducation au numérique, face aux menaces de cybersécurité. Son but : vous aider à identifier et à comprendre une tentative d'hameçonnage et de réutilisation des données.

Le message semblait crédible : un club local, une offre sportive pour vos enfants… mais il s'agissait d'un piège. Il ne fallait pas cliquer !

Rien de grave cette fois-ci. L'objectif était de montrer à quel point les cybercriminels redoublent d'inventivité pour obtenir vos informations personnelles par un simple lien.

Les risques liés au phishing sont donc nombreux :
1. L'effet boule de neige c'est à dire l'envoi de mails frauduleux à vos contacts
2. L'usurpation d'identité numérique
3. La compromission de comptes professionnels, scolaires, personnels.
4. L'atteinte à la réputation
5. Le vol de données sensibles (personnelles, bancaires ou familiales ...)

Une fois vos données saisies sur un faux site, elles peuvent être revendues ou utilisées pour usurper votre identité. Ces attaques ne concernent pas seulement les adultes, les enfants peuvent aussi en être les victimes.

Face à ce type de cybermenaces, voici quelques conseils :

1. Vérifiez l'expéditeur du message et le langage employé (caractère d'urgence, émotions, bonnes affaires)
2. Vérifiez les liens dans le courriel 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 connu), via un canal autre que celui d'origine, une adresse de messagerie peut aussi être falsifiée
6. Enfin, activez la double authentification

Si vous recherchez des conseils ou informations supplémentaires, l'application Ma Sécurité, disponible gratuitement sur les plateformes de téléchargement, est là pour vous apporter des réponses concrètes. Merci d'avoir participé à cette action. Parlez-en en famille pour protéger vos enfants.

Et si vous êtes victime d'une cybermalveillance qu'il s'agisse d'un hameçonnage, d'un piratage de comptes ou d'un virus, trouvez de l'assistance sur 17Cyber.gouv.fr

Ensemble, faisons du numérique un espace plus sûr pour nos enfants. »