
HACK Academy
PHISHING
Technique : Faire croire à la victime qu'elle s'adresse à un tiers de confiance afin de lui soutirer des renseignements personnels comme son numéro de Carte Bleue ou un mot de passe.
Ne jamais cliquer sur une pièce jointe ou sur un lien dans un e-mail qui vous semble douteux. Connectez-vous toujours via le site officiel.
Ne fournissez des informations relatives à votre CB que pour régler un achat sur un site sécurisé dont l'adresse commence par https.
Votre antivirus doit être à jour, il détectera et bloquera les programmes malveillants.
Ne jamais communiquer ses mots de passe à qui que ce soit. Utilisez un mot de passe différent sur chaque site visité, et en particulier sur son site bancaire et sa messagerie
VS DÉFIER WILLY
EN SAVOIR +


HACK Academy
VOL DE MOTS DE PASSE
Technique : Voler le mot de passe sur un site internet ou faire de nombreux essais jusqu'à trouver le bon mot de passe en allant par exemple sur les réseaux sociaux et en récoltant des infos persos sur votre vie.
Votre mot de passe ne doit pas être construit à partir d'informations publiées facilement trouvables sur les réseaux sociaux.
Créez des mots de passe les plus complexes possible et difficiles à deviner.
Utilisez un mot de passe différent sur chaque site visité qui nécessite la création d'un compte.
Ayez un anti-virus et installez un anti-spyware que vous mettrez à jour régulièrement.


HACK Academy
LOGICIELS MALVEILLANTS
Technique : Programme développé dans le but de nuire à un système informatique. Il peut être caché dans un logiciel (gratuit ou non) à télécharger ou dans une clé USB.
N'installez jamais de logiciels (gratuits ou non) qui proviennent de sources douteuses.
Installez un bon anti-virus et mettez-le régulièrement à jour afin qu'il détecte et bloque les programmes malveillants.
Ne connectez jamais une clé USB trouvée. Rapportez-la aux objets trouvés !


HACK Academy
HTTPS PAIEMENT SÉCURISÉ
Technique : Si vous vous connectez à un site web marchand non sécurisé au moment du paiement, un hacker peut très facilement récupérer les informations concernant votre Carte Bleue.
Ne saisissez JAMAIS d'informations confidentielles, et en particulier votre numéro de Carte Bleue sur la page d'un site dont l'adresse ne commence pas par «https» accompagné du cadenas.
VS DÉFIER DIMITRI
EN SAVOIR +


HACK Academy
SOCIAL ENGINEERING
Le social engineering c'est l'art d'extirper frauduleusement de l'information à l'insu de son interlocuteur en lui «tirant les vers du nez».
Restez vigilant sur les modifications de coordonnées bancaires, notamment vers des pays étrangers, ou les demandes à l'approche des congés ou de jours fériés. Demandez toujours une confirmation par un autre canal que celui demandant la modification, auprès du contact habituel du fournisseur.
Respecter les procédures de validation en vigueur dans l'entreprise. En tant que dirigeants, informez vos salariés que jamais vous n'exigerez de transgresser les procédures.
Ne donnez jamais un mot de passe à un tiers. Aucun vrai support ne vous le demandera.


HACK Academy
NAVIGATION SÉCURISÉE
Les pirates cherchent à voler des renseignements sur vous pour en faire un usage lucratif, illégal voire préjudiciable pour vous.
Limitez au strict nécessaire les informations communiquées sur Internet et n'enregistrez jamais votre mot de passe sur le navigateur internet.
Gérez la sécurité de votre navigateur grâce à l'utilisation des menus : sécurité, vie privée ou confidentialité (en fonction des navigateurs), ainsi qu'à l'emploi d'un anti-virus et d'un anti-spyware à jour.
Effacez régulièrement les cookies, l'historique de navigation, les données de formulaires ainsi que le cache du navigateur.
Lors de vos achats sur Internet, vérifiez toujours la présence du cadenas devant l'URL, symbole d'une connexion sécurisée.


HACK Academy
CONNEXION INTERNET PUBLIQUE
Restez prudent lorsque vous vous servez d'un ordinateur public ou que vous vous connectez sur un réseau public qui pourrait enregistrer toutes les informations saisies.
Si vous devez utiliser un mot de passe pour y accéder, créez en un dédié, différent de tous vos autres comptes.
Refusez l'intervention d'un tiers sur votre ordinateur, tablette ou smartphone et ne les laissez pas non verrouillés sans surveillance.
Ne vous connectez jamais à des applications bancaires, ou à votre boîte e-mail à partir d'un ordinateur public. N'en utilisez pas, non plus, pour réaliser un achat en ligne.
À partir d'un réseau public, n'installez jamais de logiciel ou de mise à jour soi-disant obligatoire et ne saisissez jamais vos coordonnées bancaires sans le «https» et le cadenas.


HACK Academy
CLÉ USB
Attention aux clés USB trouvées. Elles peuvent contenir un programme malveillant sans que cela ne soit visible.
La meilleure façon de se protéger c'est de ne jamais utiliser de clé USB d'origine inconnue.
Ayez toujours un anti-virus et un anti-spyware à jour qui détectent et bloquent les programmes malveillants (virus, chevaux de Troie, spyware...)


HACK Academy
RÉSEAUX SOCIAUX
Les pirates peuvent avoir une utilisation malveillante des informations publiées sur internet pouvant aller jusqu'à être utilisées pour réaliser des phishing ciblés.
Assurez-vous que les paramètres de sécurité sont correctement définis pour restreindre la visibilité de vos informations personnelles et de celles de votre réseau.
N'utilisez jamais d'informations que vous avez publiées sur internet dans la construction de vos mots de passe.
Ne publiez rien sur des tiers sans avoir leur consentement ceci s'appelle le droit à l'image.
N'indiquez aucune information sur votre employeur sans son accord préalable.