«Phishing» Information et prévention

Phishing classique

Dans le phishing classique, les agresseurs cherchent à attirer les victimes potentielles sur des pages Web par le moyen d'emails frauduleux et à les amener ainsi à saisir leurs données d'inscription (numéro de contrat, mot de passe, etc.) sur les pages Web falsifiées.

Vishing (hameçonnage par téléphone)

Le Vishing est une variante du phishing basée sur la communication vocale par téléphone. Comme dans le hameçonnage classique, l'utilisateur est incité, après s'être vu raconter une histoire bien ficelée, à révéler des informations confidentielles.

QR-Phishing

Dans le QR-Phishing, les agresseurs collent leurs propres codes QR conduisant à une fausse URL sur d'authentiques codes QR situés dans des lieux très fréquentés, de manière à attirer dans leur piège des utilisateurs peu méfiants. De cette manière, ils peuvent tout de suite, en particulier sur les dispositifs mobiles, démarrer des téléchargements, exécuter des scripts ou afficher une fausse page d'ouverture de session d'e-banking.

Le phishing

Le phishing ou hameçonnage désigne le vol d'informations sensibles, comme par exemple les données de connexion d'un internaute, par le biais de sites Web piratés. Le terme anglais phishing est un mot-valise composé de «password» et de «fishing» et signifie donc littéralement «pêche aux mots de passe».

Pour déjouer ces attaques, il convient d'ignorer les demandes d'identification reçues par email de la part d'un prestataire de service en ligne. De plus, il importe de vérifier lors de chaque login que la connexion est bien sécurisée par SSL.

Pour se protéger contre le phishing, ...

- ne jamais utiliser un lien reçu par email ou obtenu après avoir scanné un code QR pour se connecter à un service de banque en ligne.
- ne jamais remplir de formulaires envoyés par courriel dans lequel on demande d'indiquer ses données d'identification.
- ne jamais révéler des informations secrètes, comme par exemple les mots de passe, par téléphone.
- toujours taper manuellement l'adresse de la page de connexion de l'institut financier et vérifier la connexion SSL.
- toujours s'adresser directement à son institut financier en cas de doute.

Pour en savoir plus: www.ebas.ch/phishing

«eBanking – en toute sécurité!» informe les utilisateurs des services de banque en ligne sur les questions de sécurité

eBanking en toute sécurité!

Le site Web **www.ebankingentoutesecurite.ch** vous informe gratuitement sur les mesures nécessaires à mettre en œuvre et les règles de comportement à adopter pour une utilisation sécurisée des applications e-banking.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz