Phishing

Vol de données – voici comment se protéger

Votre Police et la Prévention Suisse de la Criminalité (PSC) – un organe intercantonal de coordination spécialisé de la Conférence des directrices et directeurs des départements cantonaux de justice et de police (CCDJP), en collaboration avec la Haute école spécialisée de Lucerne et « eBanking – en toute sécurité ! »

Un simple clic suffit…

Phishing est un néologisme d'origine anglaise qui signifie plus ou moins « aller à la pêche aux mots de passe » et qui se traduit parfois en français par « hameçonnage ». Il consiste à voler des informations personnelles et confidentielles – généralement des mots de passe.

Lors d'une attaque par **phishing,** les criminels ont recours à de faux courriels ou à des sites Internet piratés pour tenter de subtiliser des mots de passe et autres informations confidentielles telles que les numéros de cartes bancaires. Le but de l'opération est bien entendu d'en tirer un avantage financier. Les hameçonneurs visent tout particulièrement les identifiants et autres codes d'accès aux comptes de services en ligne, comme les services de banque en ligne (e-banking), les sites de vente aux enchères ou les boutiques en ligne. De plus en plus fréquemment, les messages courts tels que SMS, WhatsApp, etc. servent aussi pour des tentatives de phishing. Particulièrement perfide, ce mode opératoire nommé **smishing** (pour hameçonnage par SMS) échappe à la plupart des critères permettant de détecter les courriels de phishing.

Prise de contact

Les hameçonneurs envoient une série de faux courriels ou de messages courts en se faisant passer pour des collaborateurs de prestataires de services en ligne ou d'instituts financiers. Le contenu du message peut faire référence par exemple au fait que les informations concernant le compte ou les données d'accès (par ex. mot de passe) sont obsolètes, invitant les destinataires à cliquer sur un lien pour leur permettre de les actualiser.

Interception des données personnelles

Or le lien en question ne conduit pas sur le site officiel du fournisseur de services mais sur un site piraté, ressemblant comme deux gouttes d'eau à l'original. Tous les identifiants et mots de passe tapés sur la page de connexion contrefaite finissent directement entre les mains des malfaiteurs.

Enrichissement

Grâce aux informations volées, les criminels peuvent par exemple effectuer des virements sur leurs propres comptes ou faire des achats en ligne aux frais de la victime.

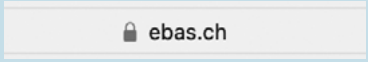
Il existe aussi une variante téléphonique du phishing, appelée **vhishing** (contraction de *voice* et de *phishing).* Les criminels se font par exemple passer pour la police ou un institut financier et inventent des histoires, afin d'obtenir des informations confidentielles.

Pour vous protéger contre le phishing et le smishing,

- ne cliquez jamais sur un lien reçu par email ou par message court, ou obtenu après avoir scanné un code QR pour vous connecter sur le site d'un prestataire de services en ligne ou d'un institut financier.
- ne remplissez jamais de formulaires envoyés par courriel ou par message court dans lesquels on vous demande d'indiquer vos informations de connexion.
- tapez toujours manuellement l'adresse de la page d'accueil du site du fournisseur de services ou de la banque dans la barre d'adresse de votre navigateur.
- lorsque la page d'accueil s'affiche, vérifiez la connexion TLS (http**s**://, cadenas, bouton de réglage) et contrôlez l'adresse Internet dans la barre d'adresse du navigateur pour vous assurer que vous êtes bien sur le bon site.

Chrome

Firefox



Safari

Edge

- en cas de doute, contactez directement le prestataire de services ou l'institut financier.

Pour vous protéger contre le vishing,

- ne transmettez jamais d'informations confidentielles à une autre personne.
- mettez fin immédiatement à tout appel téléphonique au cours duquel on requiert de vous de telles informations.

Testez vos connaissances sur le phishing en répondant aux questions du test sur l'hameçonnage « eBanking – en toute sécurité ! » sur **www.ebas.ch/phishingtest**

Vous avez reçu un email d'hameçonnage ou un message court de smishing, ou découvert un site de phishing ? Signalez-le sur le site **www.antiphishing.ch**

En savoir plus :
www.ebas.ch/phishing
www.skppsc.ch/phishing

Juin 2024

Prévention Suisse de la Criminalité
Maison des Cantons
Speichergasse 6
3001 Berne

www.skppsc.ch

Ce dépliant a été réalisé en collaboration avec la Haute école spécialisée de Lucerne et « eBanking – en toute sécurité ! »

www.ebas.ch | www.ebankingentoutesecurite.ch

HSLU Hochschule Luzern

eBanking en toute sécurité!