Eviter le phishing

Qu'est-ce que le phishing ?

Le **phishing**, traduit en français par "hameçonnage", est une méthode frauduleuse utilisée par des pirates informatiques pour voler vos données personnelles (par ex: nom d'utilisateur, mot de passe, date de naissance, numéro de carte de crédit) afin de pouvoir ensuite usurper votre identité électronique.

Une tentative de phishing se présente généralement sous forme d'un e-mail:

- qui prétend provenir d'un émetteur de confiance, comme une banque, une administration ou une entreprise
- qui utilise généralement le prétexte d'un contrôle de vos informations (menaçant même de fermer votre compte si vous ne répondez pas)
- et qui vous demande de communiquer votre nom d'utilisateur, mot de passe, numéro de carte de crédit, etc. soit par e-mail, soit en suivant un lien vers un formulaire sur un faux site web, imitant le véritable site.

Une fois en possession de vos données personnelles, les pirates peuvent accéder à vos données et usurper votre identité pour toutes sortes d'opération frauduleuses.

Comment l'éviter ?

Il faut savoir qu'aucune banque, administration ou entreprise ne vous demandera jamais par e-mail vos données personnelles. Si vous recevez un message vous demandant ce type d'information, il faut donc:

- ne jamais cliquer sur les liens contenus dans ces messages
- ne jamais répondre à ces messages

et signalez ce message à notre service de sécurité.

> Si des pirates utilisent cette technique, c'est qu'elle fonctionne encore auprès de certains utilisateurs naïfs. Les messages et les contrefaçons de sites web utilisés sont parfois très

bien imités. Vous pouvez même recevoir un message qui semble provenir de l'Unil (par exemple du helpdesk ou du centre informatique), donc faites attention. Si vous voulez accéder à un site proposé dans un lien, mais que vous n'êtes pas certain que le message provient d'un émetteur fiable, ne cliquez pas sur ce lien. Tapez plutôt l'adresse de ce lien manuellement dans votre navigateur web.

Et si cela se produit accidentellement avec votre compte utilisateur Unil

Si accidentellement vous vous laissez abuser par une tentative de phishing,
changez votre mot de passe immédiatement:

1. aller sur https://id.unil.ch/self
2. suivre les instructions.

Si vous n'êtes pas certain de savoir comment faire, appelez notre service de help desk:

021 692 22 11 (de 8h à 17h) ou par email helpdesk@unil.ch.

Créé 2019-10-29 12:56:54 UTC par Chr Gr
Mis à jour 2026-09-24 08:26:49 UTC par Chr Gr