Le vol d'identité

Le vol d'identité est une fraude visant à collecter et à utiliser de manière illégale des informations vous concernant. Le plus souvent, les informations visées sont vos identifiants. Ils permettent en effet d'accéder à votre courrier électronique et d'utiliser votre boîte mail pour envoyer des spams en usurpant votre identité.

Les moyens utilisés par les voleurs

Les techniques les plus utilisées sont l'hameçonnage et les enregistreurs de touches. Elle sont décrites par la suite.

L'hameçonnage

L'hameçonnage (ou **phishing**, et parfois **filoutage**), est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. (source: wikipedia). A l'Université, cela se traduit par des courriers électroniques vous invitant à envoyer votre nom d'utilisateur votre mot de passe sous peine de perdre l'accès à votre boîte mail, chose que l'université n'aura jamais besoin de faire. **En effet, la validité des comptes de l'Université est basée sur la base de données de la Division du Personnel. Il ne vous sera jamais demandé de prouver que vous utilisez bien votre messagerie.**

Les enregistreurs de touches

Un **enregistreur de touches** ou **Key Logger** est un programme malicieux, installé à l'insu de l'utilisateur par un virus ou une personne malintentionnée et enregistrant toute saisie effectuée sur son poste de travail. Les données ainsi capturées sont consolidées localement puis envoyées automatiquement à des pirates, et ce, en toute transparence pour l'utilisateur lésé.

Le piratage de sites tiers

De nombreux groupes de pirates exploitent des failles dans des sites commerciaux ou gouvernementaux et parviennent à récupérer les identifiants des utilisateurs. Ils peuvent ensuite utiliser ces informations pour arnaquer les utilisateurs. Notamment via des campagnes de faux chantage par courrier électronique.

Comment éviter le vol d'identité

- **Ne communiquez jamais vos identifiants**: L'Université ne vous demandera jamais vos identifiants. Quelle que soit la raison évoquée, vous devez faire preuve de prudence dès qu'il est mention de vos identifiants. Vous devez systématiquement refuser de les communiquer à quiconque, qu'il s'agisse de votre informaticien, d'un collègue ou d'un supérieur hiérarchique.
- **Vérifiez où vous saisissez vos identifiants**: Si vous êtes invité à saisir vos identifiants sur un site de l'Université, vérifiez qu'il s'agit bien d'un service officiel. L'adresse doit impérativement être de la forme **https**:quelquechose.**univ-nantes.fr** et votre navigateur doit vous indiquer que la connexion est sécurisée. Par exemple:

Firefox	
Internet Explorer	

Votre navigateur ne doit à aucun moment vous alerter sur la validité d'un certificat SSL au cours de la connexion à l'un des web services de l'Université. Tous nos certificats sont émis par une Autorité de Certification reconnue des principaux navigateurs du marché. **Une alerte sur leur validité pourrait être le signe d'une tentative d'attaque.**

- **Faites preuve de bon sens**:
  - Vérifiez l'adresse d'expédition des messages vous invitant à cliquer à entrer vos identifiants sur un site internet
  - Vérifiez l'adresse de réponse du message auquel vous répondez. S'il ne s'agit pas d'adresses universitaires, ignorez le message.
  - Ne cliquez pas sur les liens vous invitant à entrer votre mot de passe si l'adresse du lien n'est pas une adresse universitaire.
  - Le site sur lequel vous vous apprêtez à saisir vos identifiants semble-t-il affilié à l'université? Celle-ci est-elle mentionnée? le logo est-il visible?

- **Utilisez le clavier virtuel**: certains services internet de l'Université proposent un clavier virtuel vous permettant de saisir votre mot de passe à la souris et déjouant ainsi les enregistreurs de touches. Si vous êtes dans un cybercafé, chez des amis, ou encore si vous utilisez un PC auquel vous ne faites pas confiance, utilisez le clavier virtuel.

- **En cas de doute, contactez la DSIN**: Si vous rencontrez un site ou un courrier électronique suspect, si vous recevez un courrier papier ou un coup de téléphone qui vous semble douteux,

contactez la DSIN à l'adresse irts(at)univ-nantes.fr
- **N'utilisez jamais deux fois le même mot de passe**: Vos mots de passe doivent être uniques. Ne réutilisez jamais votre mot de passe Université sur des sites internet tiers et réciproquement ne réemployez pas à l'Université un mot de passe que vous utilisez par ailleurs. Si vous utilisez le même mot de passe partout, un pirate aura accès à tous les sites que vous utilisez, y compris à votre banque, à vos mails personnels, aux sites commerciaux que vous avez utilisés, etc.

* **Respectez la politique des mots de passe de l'Université**

Conséquences du vol d'identifiant

Pour la victime

En général, la première chose que fera le voleur c'est utiliser les identifiants de sa victime pour se connecter à son compte via le webmail:

- il pourra y lire la correspondance de la victime pour en récupérer de nouvelles informations: coordonnées bancaires, autres identifiants, etc
- il utilisera les données personnelles de la victime pour s'enrichir au maximum, soit en revendant ces informations (liste des contacts, coordonnées bancaires, données concernant le travail de recherche de la victime, ...), soit en les exploitant lui-même. Il se connectera aux sites commerciaux que la victime a l'habitude d'utiliser, utilisera son compte pour commander des objets de valeur, etc.
- le compte sera utilisé pour envoyer des millions de spams.

Chantage aux données intimes

En 2018 une nouvelle forme d'exploitation des identifiants volés a émergé: **le chantage par courrier électronique.**

Le maître chanteur va contacter la victime en lui faisant croire qu'il a le contrôle du poste de travail de l'utilisateur. Pour le prouver le pirate présente parfois un mot de passe de l'utilisateur issu d'un piratage de sites commerciaux ou gouvernementaux (dailymotion en 2006, Adobe en 2013, linkedin en 2016, etc.). Il va prétendre posséder des données intimes qu'il menace de divulguer si l'utilisateur ne paie pas.

Parfois le courrier semble avoir été envoyé avec l'adresse de l'utilisateur, le pirate s'en servant pour faire croire qu'il a bien le contrôle du poste de travail.

Il est bien sur faux que le maître chanteur contrôle l'ordinateur et des données personnelles de l'utilisateur. En effet le mot de passe présenté à l'utilisateur ne provient pas d'un quelconque virus ou outil de piratage installé sur le poste de l'utilisateur mais du piratage d'un site internet. Il est donc sain d'ignorer la menace et de supprimer le courrier. De plus l'adresse d'expédition d'un courrier électronique n'a pas plus de valeur que celle que vous écrivez au dos d'un courrier papier: il est possible d'y mettre l'adresse que vous voulez.

Il est parfois possible d'identifier le site internet piraté ayant mené à la divulgation du mot de passe

utilisé. Troy Hunt, un expert en sécurité, a mis en place un site internet vous permettant de vérifier si vos identifiants ont été obtenus lors d'un piratage: https://haveibeenpwned.com/

Pour l'Université

Contrairement à ce que certains pourraient penser, le vol d'identifiant concerne tout le monde. Si une personne se fait voler ses identifiants, non seulement la personne est victime mais toute l'université en sera victime aussi:

- le voleur pourra spammer en utilisant les serveurs de l'université, entrainant la catégorisation de l'établissement comme spammeur. Les courriers électroniques envoyés de l'université, considérés comme spams potentiels, seront alors refusés par le reste du monde.
- le voleur pourra accéder aux données de la victime ainsi qu'à tous ses partages. Les données de son laboratoire seront alors compromises.
- si vous avez échangé des données confidentielles avec la victime, celles-ci pourront alors être utilisées contre vous.

Aller plus loin

L'ANSSI (L'Agence Nationale de ls Sécurité des Systèmes d'Information) rappelle dans cette note les règles élémentaires de sécurité pour la réception des courriels : 5 réflexes à avoir lors de la réception d'un courriel

- *N'ayez pas une confiance aveugle dans le nom de l'expéditeur*
- *Méfiez-vous des pièces jointes*
- *Ne répondez jamais à une demande d'informations confidentielles*
- *Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français dans le texte ou de la langue pratiquée par votre interlocuteur*
- *Paramétrez correctement votre logiciel de messagerie*

Lire la note.