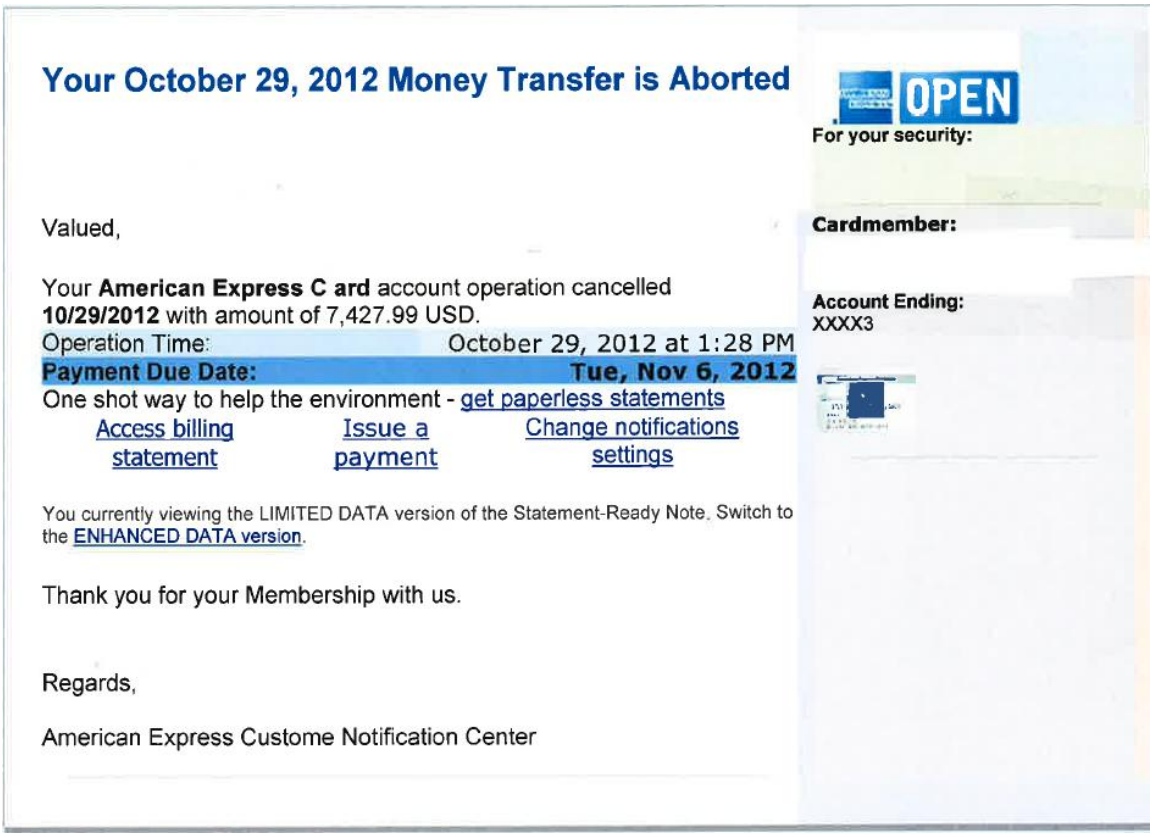
info·SIRCO
ENQUÊTE ET PROTECTION
Novembre 2012

Le *phishing* : Toujours un problème ?

Alors qu'on pensait que le phishing était un mauvais souvenir, force est de constater qu'il s'agit encore d'un problème récurrent de sécurité des données des particuliers. En effet, il s'agit d'un moyen habile de vol de données qui utilise spécialement les faiblesses humaines (social engineering) plutôt que les faiblesses techniques.

Exemple de *phishing* agressif reçu par courriel par un confrère:



Your October 29, 2012 Money Transfer is Aborted

OPEN

For your security:

Valued,

Your **American Express C ard** account operation cancelled **10/29/2012** with amount of 7,427.99 USD.

Operation Time: October 29, 2012 at 1:28 PM

Payment Due Date: Tue, Nov 6, 2012

One shot way to help the environment - get paperless statements

Access billing statement | Issue a payment | Change notifications settings

You currently viewing the LIMITED DATA version of the Statement-Ready Note. Switch to the ENHANCED DATA version.

Thank you for your Membership with us.

Regards,

American Express Custome Notification Center

Cardmember:

Account Ending: XXXX3

Il s'agit d'un vrai compte American Express. Cet exemple réel démontre que le fraudeur a en sa possession des informations personnelles précises concernant notre confrère : Son nom et prénom, son adresse courriel et l'information de la carte American Express.

L'exemple témoigne d'une base de donnée « x » qui a été fragilisée afin d'obtenir les informations. Et comme expliqué plus bas, le courriel amène la victime à cliquer sur un programme exécutable « ENHANCED DATA version » afin que cette dernière y valide certaine information en toute confiance.

Rappel : Qu'est-ce que le *phishing*?

Le *phishing*, ou hameçonnage, consiste à amener la victime sur une page Web, ou sur un fichier joint à un courriel afin de pouvoir récupérer ses données. Pour ce faire, le pirate crée une copie très ressemblante d'une institution connue, afin que la victime dupée y transmette des informations en toute confiance.

La faille humaine est particulière exploitée dans ce type de piratage puisqu'on fait croire à la victime qu'elle se trouve sur un site légitime. Alors que la plupart des individus estiment qu'ils ne tomberaient pas dans le piège, une étude réalisée en mai 2012 par KaperskyLab démontre en effet que 50 % des personnes interrogées se disent incapables de reconnaître un message de *phishing*.

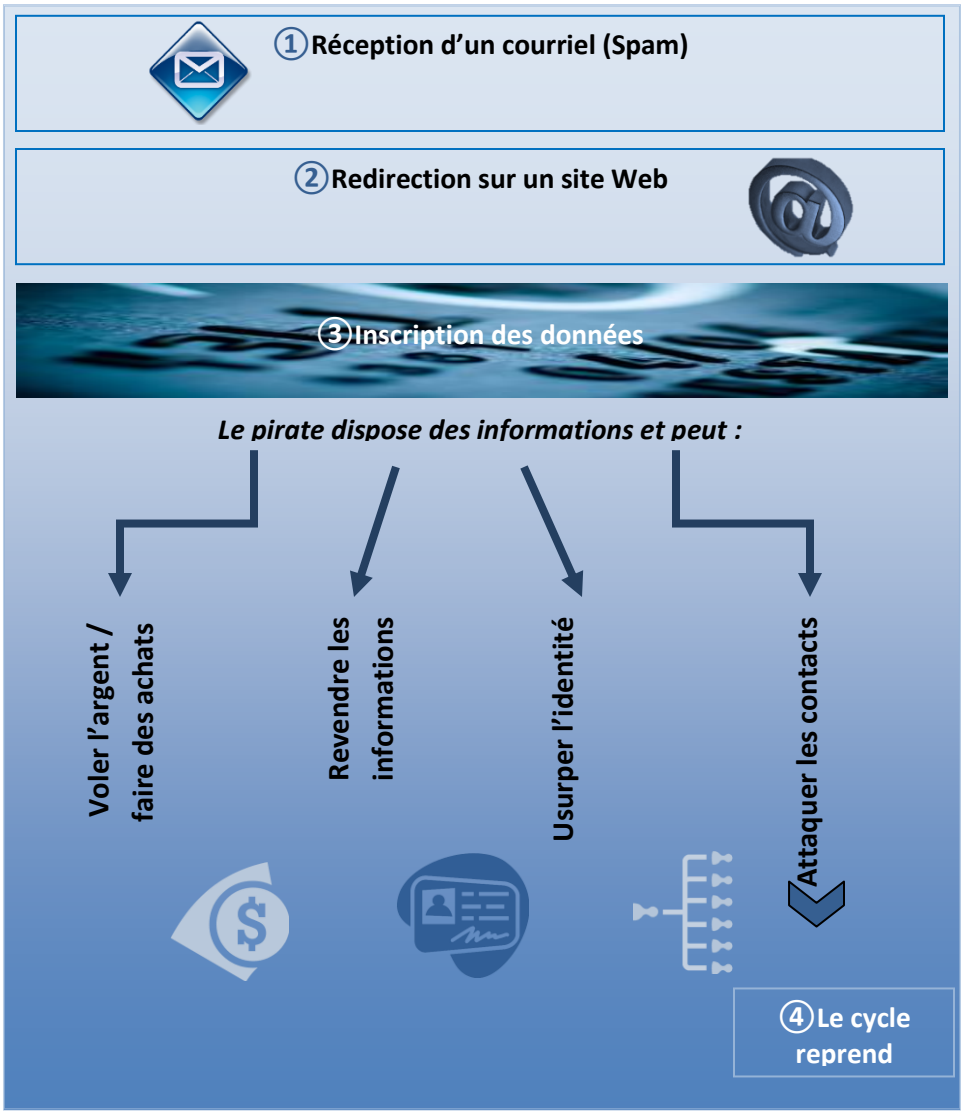
« 50 % des personnes se disent incapables de reconnaître un *phishing* »

Les attaques par *phishing* augmentent, car se diversifient. On constate qu'en plus d'utiliser la messagerie, le *phishing* se répand maintenant sur les réseaux sociaux ou encore les téléphones intelligents, car ce sont aujourd'hui les moyens de communication les plus répandus.

Il existe plusieurs types de *phishing* :

Type	*Objectifs*	*Moyens*	*Risques*	*Complexité*
Identité bancaire	Récupérer les données bancaires : Login des banques en ligne/ Code secret/ carte de crédit…	Tromper l'individu en se faisant passer pour une institution bancaire	Élevé sur la fréquence Achat frauduleux revendu pour récupérer de l'argent (western union, coin star, …)	Connaissance en informatique élevée (création et piratage site Web) *Profil* : Jeunes, étudiants en informatiques
« Stolen data »	Récupérer le numéro de carte de crédit dans le but de revendre cette information sur le marché noir de la cybercriminalité	Tromper l'individu en se faisant passer pour un service (télécommunication)	En expansion sur la fréquence Clonage de carte de crédit	Connaissance en informatique élevée *Profil* : Crime organisé dans les réseaux de cybercriminalité
Identité virtuelle / spam et scam	Récupérer des informations personnelles dans le but d'usurper l'identité.	Tromper l'individu sur des copies de site de réseaux sociaux ou service de courriel	En expansion sur la fréquence Extorsion d'argent ou récupération des contacts pour diffuser l'attaque.	Connaissance en informatique faible.

Description d'une attaque par *phishing* :



À propos: CONFÉRENCE SUR LES MÉDIAS SOCIAUX – 26 NOVEMBRE 2012 – CINEMA EXCENTRIS

Conférence animée par *Me Rhéaume Perreault*, CRIA, Heenan Blaikie et *Claude A. Sarrazin*, président et fondateur de SIRCO.

Ce colloque aborde pendant une demi-journée deux aspects essentiels et inhérents aux médias sociaux dans le monde du travail :

- Connaître les médias sociaux : un must en gestion des ressources humaines
- Les médias sociaux : une source infinie de renseignements !