QUE FAIRE EN CAS DE TENTATIVE DE FRAUDE OU DE FRAUDE AVÉRÉE ?

Commission Systèmes d'information – Sécurité

Octobre 2014

Commission
Système d'information – Sécurité
Octobre 2014

QUE FAIRE EN CAS DE TENTATIVE DE FRAUDE OU DE FRAUDE AVÉRÉE ?

- ✓ La protection des données
- ✓ Les réflexes à avoir
- ✓ Les bonnes pratiques
- ✓ Quelques numéros utiles de Directions de la police judiciaire

La protection des données (1/3)

Il n'est pas rare de recevoir des e-mails d'inconnus demandant de saisir des informations personnelles (codes d'accès, coordonnées bancaires, …) ou de cliquer sur des liens. Ces attaques visant souvent les systèmes personnels suscitent la plupart du temps la méfiance.

Des attaques plus élaborées, du même type, visant les systèmes d'information de l'entreprise, sont de plus en plus fréquentes. Le contenu de ces e-mails est généralement formulé de façon à inciter à cliquer sur un lien ou à activer une pièce jointe. Il faut être particulièrement vigilant : dès lors qu'une pièce jointe ou un lien envoyé par un pirate expéditeur est activé, des programmes malveillants peuvent être installés et devenir une menace pour le système d'information de l'entreprise.

La protection des données (2/3)

Quelques bonnes pratiques pour faire face aux attaques ciblées par e-mail sont recensées ci-après en fonction de critères simples :

Expéditeur :

- ✓ Connaissez-vous l'expéditeur ? Son adresse paraît-elle habituelle ?
- ✓ Si vos collègues vous contactent normalement en utilisant leurs adresses professionnelles, il n'est pas normal qu'ils vous fassent des demandes depuis une toute autre adresse.

•

Liens :

- ✓ Ne jamais ouvrir un lien venant d'un expéditeur que vous ne connaissez pas.
- ✓ Ne pas cliquer sur les liens lors de la lecture d'un message sur votre Smartphone.
- ✓ Sur votre PC, vous pourrez survoler le lien avec votre souris pour voir s'il dirige vers le site prétendu. Si ce n'est pas le cas, ou même si le site vous est inconnu ou paraît suspect pour tout type de raison (orthographe approximative, adresse fantaisiste, etc.), ne suivez surtout pas le lien.

•

Pièces jointes :

- ✓ Ne jamais ouvrir une pièce jointe venant d'un expéditeur que vous ne connaissez pas.
- ✓ Si vous devez ouvrir des pièces jointes reçues par email, effectuez cette action sur votre poste de travail uniquement car il est protégé par un antivirus.

La protection des données (3/3)

•

Canulars :

- ✓ De nombreux canulars circulent sur Internet. Au-delà des rumeurs ou informations fantaisistes, ils véhiculent également souvent des menaces pour les systèmes informatiques.
- ✓ Des sites recensent les canulars pour vous aider à les identifier, par exemple www.hoax-slayer.com ou www.hoaxbuster.com.
- ✓ Ne relayez pas les messages reçus sans vous être assurés au préalable du sérieux de leur contenu.

•

Texte :

- ✓ Evaluez la qualité du texte et des images.
- ✓ Les fautes d'orthographe ou de grammaire doivent éveiller vos soupçons.
- ✓ Les offres atypiques non sollicitées doivent être traitées avec la plus grande vigilance.

•

Répondre :

- ✓ Si tout paraît authentique jusque-là, posez-vous les questions suivantes avant de fournir les informations qui vous sont demandées par e-mail :
  - **Mon correspondant est-il celui qui est supposé me demander ces informations ?**
  - **Mon correspondant a-t-il un réel besoin métier d'avoir ces informations ?**
  - **Suis-je habilité à communiquer ces informations ?**
- ✓ Ne fournissez les informations que si vous êtes en mesure de répondre OUI à l'ensemble de ces questions. En cas de doute, n'hésitez pas à contacter votre Service système d'information ou votre hotline, ainsi que votre hiérarchie.

Les reflexes à avoir (1/2)

Les fraudeurs ? De vrais experts !

- ✓ Ils connaissent parfaitement le fonctionnement de votre société.
- ✓ Ils savent parfaitement imiter les signatures.
- ✓ Ils ont une parfaite maitrise de la falsification de documents (papier à entête, …).
- ✓ Ils ont une parfaite maitrise des outils pour imiter une voix, un e-mail interne.
- ✓ Ils ont une vraie connaissance et une vraie stratégie d'attaque des fragilités dans l'organisation de l'entreprise (achat-vente d'une filiale, changement de gouvernance, changement de PDG, mouvements sociaux, …).
- ✓ Ils demandent la confidentialité absolue.
- ✓ Et ils ont l'audace, la persévérance et la capacité de manipuler un interlocuteur.

Les reflexes à avoir (2/2)

Quelques exemples de fraude

- ✓ Faux ordre de virement papier.
- ✓ Faux ordre de virement par fax.
- ✓ Demande urgente par téléphone d'un virement dans le cadre d'une acquisition qui doit rester confidentielle, en se faisant passer pour le dirigeant de l'entreprise.
- ✓ Demande au service comptable d'exécuter un virement à l'étranger afin de démasquer un escroc, en se faisant passer pour le dirigeant de l'entreprise et en précisant que cette demande rentre dans le cadre d'une enquête de la brigade financière et que la confidentialité doit être assurée.
- ✓ Demande de modification d'un RIB fournisseur par téléphone, confirmée par un faux mail émanant de la bonne adresse e-mail dudit fournisseur.
- ✓ Demande urgente de virement par téléphone, avec utilisation d'un synthétiseur de voix.
- ✓ Demande d'émission de virement pour tester les fichiers au format SEPA en se faisant passer pour une banque de l'entreprise.
- ✓ Falsification de courriers électroniques ou de documents papier en se servant d'informations recueillies sur internet (logo, adresse, fax, mail et même signature des dirigeants).
- ✓ Utilisation de techniques permettant de faire apparaître des numéros de téléphone français alors que ces appels émanent de l'étranger.
- ✓ Utilisation de technologies permettant de pirater des adresses e-mail (fournisseurs, dirigeants de l'entreprise) alors que ces messages émanent des boites e-mail des fraudeurs.
- ✓ Usurpation d'identité après collecte des données personnelles pour confirmer les paiements frauduleux.
- ✓ Falsification de factures fournisseurs.

Les bonnes pratiques (1/3)

AVANT

Si vous ne voulez pas être victime d'une fraude, vous devez :

- Sensibiliser vos équipes ;
- Mettre en place un dispositif de contrôle interne pertinent et revu de façon régulière -> voir cahier technique publié par l'AFTE en octobre 2013 ;
- Mettre en place des procédures strictes d'émission des moyens de paiement en privilégiant l'électronique et en évitant le papier (courrier, fax) même si un contre-appel est prévu avec la banque ;
- Hiérarchiser les pouvoirs internes (ouverture d'un compte tiers, modification d'un compte bancaire) et les pouvoirs bancaires en favorisant la séparation des tâches ;
- Demander à vos banques de mettre en place des procédures plus efficace qu'un simple contre-appel pour tout type de paiement non conforme ;
- Privilégier la spécialisation des comptes bancaires par type de flux, ce qui permet à la banque d'identifier plus facilement les opérations anormales

Les bonnes pratiques (2/3)

PENDANT

Si vous avez identifié une fraude en cours, vous devez :

- Alerter immédiatement votre Direction Générale et votre service sécurité et/ou informatique et/ou audit ;
- Si demande de connexion via internet à un système ou d'activation d'un lien, ne surtout pas se connecter ;
- Jouer le jeu en simulation afin d'obtenir un maximum de renseignements (IBAN, pays, nom, etc.) ;
- Prévenir la banque concernée.

Les bonnes pratiques (3/3)

APRÈS

Si vous avez été victime d'une fraude, vous devez :

- Alerter immédiatement votre Direction Générale et votre service sécurité et/ou informatique et/ou audit ;
- Contacter la banque concernée pour (1) signaler la fraude et (2) si possible, stopper l'ordre de paiement ;
- Déposer une plainte (en collaboration avec votre banque) auprès de la police et du procureur de la République ;
- Lancer un audit pour (1) vérifier l'étendue de la fraude et (2) son mode opératoire ;
- Mettre en place ou réactiver les procédures contre la fraude.

Quelques numéros utiles de Directions de la police judiciaire

Paris et petite couronne (dpt 92, 93, 94) :

Brigade Fraude aux Moyens de Paiements (BFMP) 01 55 75 22 94

Lille - Division Economique et Financière de la Direction Interrégionale de la Police Judiciaire : 03 20 10 78 00

Ouest :

Direction Interrégionale Police Judiciaire

Bretagne	Philippe CAMPANA	02.99.79.87.50	philippe.campana@interieur.gouv.fr
Angers	Yohann SALMON	02.41.57.54.11	yohann.salmon@interieur.gouv.fr
La Rochelle	Denis JOUVET	06.86.13.17.87	denis.jouvet@interieur.gouv.fr
Nantes	Miguel GHESQUIÈRE	02.53.46.75.50	miguel.ghesquiere@interieur.gouv.fr
Poitiers	Bruno RUTAULT	06.75.69.62.11	bruno.rutault@interieur.gouv.fr

Autres régions : en cours de mise à jour

Remerciements et Contact

L'AFTE remercie les membres de la commission Systèmes d'information – Sécurité ayant contribué à ce document.

Adresse de contact : valerie.voisin@afte.com