Tendances en matière de fraude

Contrôles de sécurité en ligne HSBC*net*

HSBC*net*

HSBC

Table des matières

- Types de fraudes
  - Attaques de logiciels malveillants
  - Piratage de messageries professionnelles
  - Phishing vocal (« vishing »)
  - Phishing par SMS (Short Message Service) (« smishing »)
- Comment éviter de se faire escroquer
- Sécurisation renforcée des services bancaires en ligne HSCC*net*

Attaques de logiciels malveillants

- Un logiciel malveillant est un programme qui perturbe le fonctionnement de l'ordinateur dans le but de recueillir des informations sensibles ou d'accéder à des systèmes

- Les systèmes du client sont piratés afin de réaliser des transactions frauduleuses

- La vitesse d'exécution de l'ordinateur est ralentie ; des pages inhabituelles apparaissent à l'écran demandant à l'utilisateur de saisir des codes ou l'informant qu'il devra attendre un certain temps avant de pouvoir se reconnecter

- Un clic accidentel sur un lien dans un mail de phishing, sur un site corrompu ou vers un logiciel piraté peut déclencher le téléchargement d'un programme malveillant

HSBC

Attaques de logiciels malveillants

Exemples :

- Une page « ***Veuillez patienter*** » apparaît au moment de la connexion
- L'ordinateur semble particulièrement lent
- Une fenêtre contextuelle s'ouvre avec un message demandant à l'utilisateur de saisir le code de sécurité ou d'appuyer sur le bouton jaune
  (demande de validation de jeton, vérification de la sécurité ou resynchronisation)
- Un message indique qu'un deuxième utilisateur doit se connecter sur le même ordinateur pour valider

Piratage de messageries professionnelles

- Moyen d'arnaquer les clients d'institutions financières
- Se produit lorsque l'escroc se fait passer pour un sous-traitant, un fournisseur, un créancier ou même un membre de la direction et demande à une entreprise de modifier ses paramètres de paiement
- Les paiements ultérieurs seront alors redirigés vers le compte de l'escroc

Pourquoi ce type d'attaques est-il difficile à détecter ?

- Aucune institution financière n'est épargnée par ces attaques qui ne sont pas non plus spécifiques de certains pays ou régions
- Les escrocs se préparent avant de passer à l'attaque, en menant des activités de reconnaissance (ingénierie sociale) permettant de cibler avec exactitude les noms et coordonnées utilisés
- Les adresses e-mail utilisées pour les demandes de modification du compte d'un bénéficiaire sont identiques ou très semblables à celles des fournisseurs, ce qui rend la fraude difficile à détecter
- Il est déjà arrivé que des escrocs piratent le compte de messagerie d'un créancier afin d'envoyer une demande de modification du bénéficiaire qui semble alors tout à fait légitime
- Les escrocs envoient par la poste de fausses lettres qui paraissent provenir du créancier
- Exploite une réaction ou un comportement humain que la technologie ne peut pas prévenir

HSBC

Piratage de messageries professionnelles

Exemples :

- Des e-mails de fournisseurs, nouveaux ou existants, prétendant que le numéro de compte a changé et demandant à ce que le paiement soit dorénavant versé dans une autre banque ou sur un autre compte
- Des fournisseurs qui prétendent qu'il faut maintenant effectuer les paiements à la société mère, dans un autre pays
- Des employés qui reçoivent un e-mail de leur PDG ou de leur directeur financier leur demandant d'effectuer un paiement ; il s'avérera ensuite que le compte de messagerie du PDG ou du directeur financier a été piraté
- Les e-mails peuvent provenir d'un domaine qui ressemble à une source légitime

Phishing vocal (« vishing »)

- Le terme « vishing » décrit les tactiques que les fraudeurs utilisent pour récupérer des informations personnelles par téléphone (telles que des identifiants de sécurité liés à des services bancaires en ligne).
- Les fraudeurs peuvent contacter les clients en se faisant passer pour HSBC. Ils peuvent vous demander d'exécuter des actions permettant de réaliser des paiements non autorisés destinés au criminel, notamment fournir des codes de sécurité générés par votre jeton.

HSBC ne vous demandera jamais d'informations pouvant être utilisées pour effectuer un paiement (comme un code de dispositif de sécurité ou des informations de sécurité).

HSBC

Phishing par SMS (« smishing »)

- Le smishing est une variante du phishing qui utilise des messages SMS au lieu d'e-mails
- Les fraudeurs peuvent contacter les clients par SMS en se faisant passer pour HSBC. Ils peuvent vous demander d'exécuter des actions permettant de réaliser des paiements non autorisés destinés au délinquant, notamment fournir des codes de sécurité générés par votre jeton.

HSBC ne vous demandera jamais d'informations pouvant être utilisées pour effectuer un paiement (comme un code de dispositif de sécurité ou des informations de sécurité)

HSBC

Comment pouvez-vous éviter de vous faire escroquer ?

- Méfiez-vous des demandes de modification d'informations concernant le bénéficiaire ; demandez une explication pour chaque modification et confirmez toujours les modifications par d'autres moyens
  (c.-à-d. rappelez, ne répondez pas directement à l'e-mail)

- Établissez des procédures de contrôle en interne à suivre en cas de demandes de modification des coordonnées du bénéficiaire

- Si des fenêtres inhabituelles s'ouvrent ou si votre ordinateur est anormalement lent, déconnectez-vous complètement de HSBC*net* puis exécutez la toute dernière version de votre logiciel de protection antivirus. En cas de doute, contactez votre service informatique ou le service clientèle de HSBC.

- Sensibiliser les collaborateurs aux risques de fraude

...Comment pouvez-vous éviter de vous faire escroquer ?

- Ne divulguez jamais d'informations de sécurité par téléphone lors d'appels non sollicités (c.-à-d. votre nom d'utilisateur, les informations de votre jeton ou les données de paiement)

- Si vous recevez un appel non sollicité de la part de HSBC, prenez les coordonnées de la personne qui vous appelle, puis confirmez ces informations auprès du service clientèle ou d'assistance de HSBC

- Ne procédez à aucune modification des données de paiement si vous n'êtes pas certain que la demande est légitime

- Signalez toute tentative de fraude à votre banque et modifiez les paramètres de votre messagerie (c.-à-d. changez votre mot de passe)

HSBC

Sécurisation renforcée des services bancaires en ligne HSBC*net*

- N'appuyez jamais sur le bouton jaune de votre dispositif de sécurité, sauf pour signer une transaction que vous avez créée vous-même ; HSBC ne vous demande jamais d'appuyer sur le bouton jaune au moment de la connexion
- Utilisez le double contrôle pour les transactions et les accès (*c.-à-d. qu'il faut au moins deux personnes pour réaliser une activité*)
- Téléchargez le logiciel Webroot *SecureAnywhere* sur www.hsbcnet.com sans frais
- Définissez des limites de signatures
- Bloquez les connexions qui ne proviennent pas d'une liste d'adresses IP autorisées
- Mettez à jour les logiciels qui ne sont plus pris en charge par vos fournisseurs (*p.ex. Internet Explorer 7*)
- Accédez toujours à HSBC*net* en insérant l'adresse du site Web dans la barre d'adresse de votre navigateur
- N'utilisez jamais les liens qui apparaissent dans le corps d'e-mails pour y accéder ; ne vous fiez pas uniquement à l'apparence d'un site Web lorsque vous utilisez HSBC*net*

HSBC