Ne soyez pas la proie du hameçonnage

Cliquer sur des liens vers des sites Web factices peut conduire à des vols de données en ligne

Pour attraper des poissons, on utilise un appât. Les voleurs en ligne qui pratiquent le hameçonnage sur le Web aiment aussi se servir d'appâts.

Le hameçonnage consiste à envoyer un courrier électronique ou un message instantané qui semble provenir d'une société réelle et fiable — mais c'est un piège. Les escrocs en ligne qui se livrent à ces activités espèrent amener leur lecteur à cliquer sur un lien contenu dans le message.

Si un employé vient à mordre à l'hameçon, deux choses peuvent se produire, aussi mauvaises l'une que l'autre. Le lien pourra amener cette personne sur un site Web ou une fenêtre contextuelle crédible (mais factice) dont le but est de se faire passer pour la société contrefaite. Cette personne pourra également être poussée à appeler un numéro de service à la clientèle. Dans les deux cas, on demandera à l'employé de divulguer des informations personnelles sensibles telles que des numéros de compte bancaire ou de carte de crédit, des mots de passe ou des codes secrets — tous pouvant être utilisés pour accéder à son compte ou usurper son identité. Une société d'étude estime que les pertes directement attribuables au hameçonnage se sont élevées à 137 millions de dollars en 2004.

L'autre éventualité est qu'en cliquant sur le lien, des logiciels espions pourraient s'installer sur l'ordinateur de la victime. Les logiciels espions peuvent enregistrer toute information saisie au clavier et voler des informations sensibles à mesure qu'elles sont tapées. Ces programmes qui surveillent la frappe peuvent attendre que vous consultiez votre le site de votre institution financière, votre messagerie électronique ou autres comptes en ligne et envoyer les mots de passe et les numéros de compte à l'escroc à l'autre bout de la ligne. Muni d'identifiants et de mots de passe, le voleur pourra se servir de techniques de piratage classiques pour accéder non seulement à l'ordinateur détourné, mais à tout le réseau de l'entreprise.

Tout employé qui est victime d'une escroquerie au hameçonnage peut mettre son compte en banque et son crédit, voire son identité, en danger. Mais votre entreprise peut perdre encore plus.

Si des cyber-voleurs se servent de technologies de piratage pour accéder aux réseaux de l'entreprise par l'intermédiaire de l'ordinateur détourné d'un employé, ils peuvent dérober des informations internes comme des listes de diffusion ou autre propriété intellectuelle. Le vol des renseignements confidentiels de vos clients pourrait avoir un impact désastreux sur votre entreprise en détruisant la confiance qu'ils témoignent à votre entreprise et à votre marque.

Quelques conseils

Méfiez-vous d'une nouvelle forme de falsification appelée «*pharming*», dans laquelle les voleurs modifient le système qui achemine le trafic Internet vers un site particulier. Les escrocs du pharming mettent en place des sites Web jumeaux factices et, en exploitant des vulnérabilités dans le Web lui-même, détournent les utilisateurs des sites commerciaux légitimes qu'ils voulaient visiter.

Quatre conseils pour ne pas se faire attraper

Étant donné les dommages potentiels, il convient d'agir afin de protéger votre entreprise d'une attaque de hameçonnage. Voici quatre méthodes pour ce faire.

1. Vérifiez que les ordinateurs de votre entreprise sont à jour
Vous devriez disposer des systèmes de sécurité de base pour les ordinateurs et le réseau. Cela signifie qu'un antivirus doit être installé sur tous les ordinateurs de votre réseau, et que votre réseau et tous les ordinateurs qui y sont connectés soient protégés par un pare-feu Internet. Un pare-feu dresse une barrière de protection entre votre réseau et Internet.

Veillez à toujours garder vos logiciels à jour. Téléchargez régulièrement les dernières mises à jour pour votre programme anti-logiciels espions et votre antivirus. La plupart des programmes peuvent procéder à une analyse automatique de votre système. Vous pouvez visiter Microsoft Update (lien US) pour recevoir les mises à jour hautement prioritaires pour Windows, Office et les autres programmes Microsoft. Windows XP Service Pack 2, notamment, empêche l'affichage des adresses Web frauduleuses pour que vous puissiez vérifier la véritable source du site que vous visitez.

2. Réduisez votre vulnérabilité
Commencez par utiliser des filtres pour bloquer les courriers électroniques de hameçonnage avant qu'ils n'atteignent vos employés. Si vous utilisez Outlook 2003, vous pouvez définir le filtre anti-courrier indésirable pour contrôler la nature des messages qui arrivent dans votre boîte de réception. Le filtre détermine automatiquement si un message doit être traité comme indésirable en fonction de plusieurs facteurs. Si vous utilisez Exchange Server 2003, vous pouvez vous servir d'autres filtres anti-courrier indésirable.

Pour bloquer dans votre navigateur les fenêtres intempestives qui pourraient être des arnaques au hameçonnage, installez un logiciel de blocage comme MSN Pop-up Guard ou celui intégré à Windows XP Service Pack 2.

3. Formez vos employés
Même les experts en fraude par courrier électronique peuvent avoir des difficultés à distinguer une arnaque bien réalisée d'un message authentique. C'est pourquoi protéger vos employés du hameçonnage nécessite de la vigilance, des précautions et des connaissances.

Commencez par établir une stratégie d'utilisation d'Internet qui précise quand le personnel peut naviguer

sur le Web à des fins personnelles et expliquez clairement quelles activités y sont interdites. Apprenez également à vos employés qu'ils ne doivent jamais donner de renseignements personnels dans un message électronique, un message instantané ou une fenêtre intempestive. La plupart des entreprises de confiance n'utilisent pas ce genre de méthodes pour obtenir des données confidentielles.

De plus, vos employés doivent savoir qu'il ne faut pas cliquer sur un lien dans un courriel, un message instantané ou une fenêtre intempestive qui demande des renseignements personnels, sinon ils risquent d'être amenés sur un site factice où les renseignements qui seront données peuvent être envoyés à un escroc. Conseillez à vos employés qui ne sont pas sûrs de l'authenticité d'un courriel de rechercher le numéro de la société sur un document papier ou dans l'annuaire et de l'appeler. Pour visiter le site Web, tapez l'adresse ou utilisez vos Favoris.

4. Assurez-vous que le site Web protège les données sensibles
Les escrocs au hameçonnage peuvent falsifier les adresses Web affichées par le navigateur. Si vous avez le moindre doute sur la légitimité d'un site, soyez prudent et quittez-le.

Si vous pensez que le site est authentique, il est quand même préférable de vous assurer de quelques critères avant de soumettre des données financières ou personnelles. Par exemple, regardez si https («s» pour sécurisé) s'affiche dans l'adresse Web, au lieu de http seulement. Cherchez aussi un petit cadenas fermé ou une clé intacte dans la barre des tâches, tous deux signe d'un chiffrement des données, une mesure de sécurité qui protège les données sensibles lorsqu'elles transitent par Internet.

Regardez le cadenas de plus près. Double-cliquez dessus pour afficher le certificat de sécurité du site. Cherchez la concordance entre le nom dans l'adresse Web et sur le certificat de sécurité; si le nom est différent, vous êtes peut-être sur un site factice.

Pour vous informer sur les dernières arnaques au hameçonnage et leurs statistiques, visitez le Anti-Phishing Working Group (lien US), une association dont le but est d'éradiquer les fraudes en ligne et le vol d'identité.

Haut de la page