Guides de sécurité pour les petites entreprises

Ingénierie sociale : **pirater les personnes, et non les machines**

AVG AU TRAVAIL

Ingénierie sociale :
pirater les personnes, et non les machines

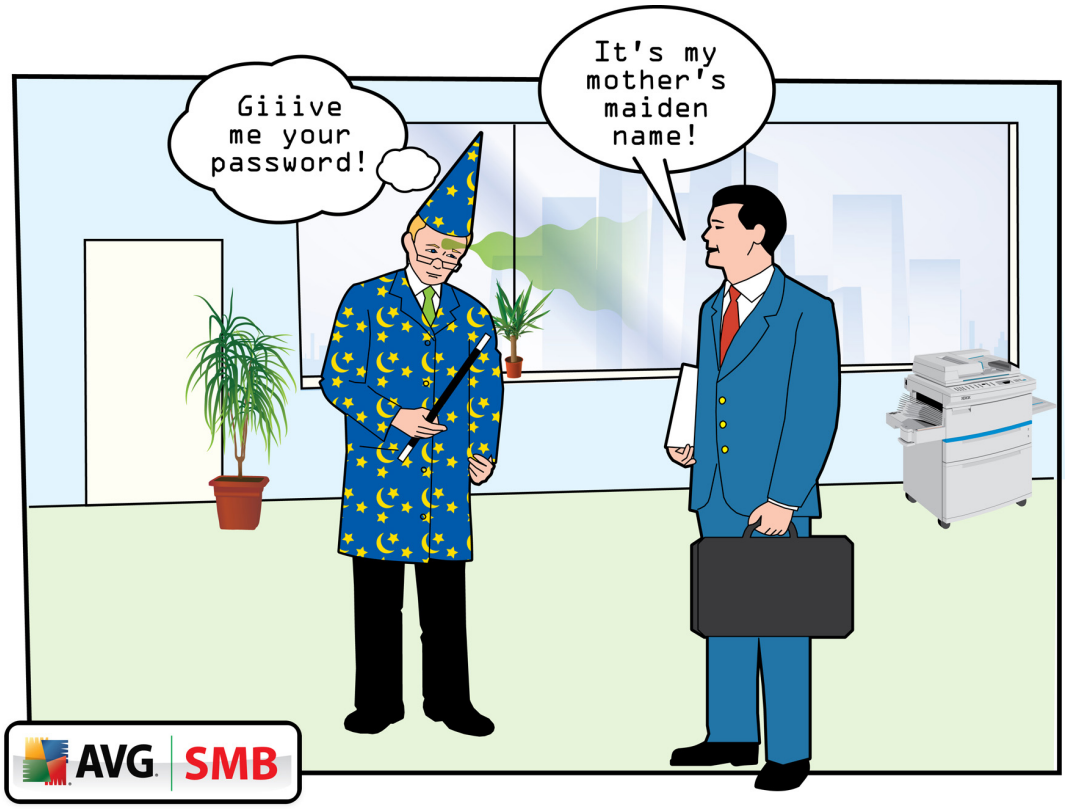
Le maillon faible de tout système informatique est presque toujours l'être humain qui l'utilise : les criminels et les pirates ne le savent que trop bien.

L'ingénierie sociale est extrêmement répandue et souvent efficace…

- Des spécialistes de la sécurité ont facilement convaincu des employés de leur communiquer leur mot de passe en échange d'un stylo gratuit
- Plus de la moitié des utilisateurs d'ordinateurs interrogés au cours d'une enquête récente réalisée par AVG avaient reçu des e-mails de hameçonnage

Les pirates sont souvent décrits comme des génies de la technologie qui utilisent des codes informatiques diaboliquement complexes. Même si c'est en partie vrai, accéder à un ordinateur peut être aussi simple que persuader quelqu'un de révéler son mot de passe. Cette tactique d'exploitation de « l'aspect humain » de l'utilisation des ordinateurs est appelée ingénierie sociale et est largement reconnue comme l'une des techniques les plus efficaces utilisée par les cybercriminels. « L'être humain est souvent le maillon faible de la chaîne de sécurité, avertit le site de conseil du gouvernement StaySafeOnline. « Les criminels et les escrocs le savent et s'en servent. » Découvrez comment repérer les tactiques qu'ils emploient. »

Il est facile de se laisser berner



Il faut se méfier de choses très simples comme les appels téléphoniques sur un poste choisi au hasard pour inciter la personne qui répond à révéler son mot de passe sur le réseau à l'aide de questions apparemment anodines. « Si un pirate ne parvient pas à recueillir suffisamment d'informations auprès d'une source, il ou elle peut contacter une autre source dans la même entreprise et utiliser les réponses de son premier interlocuteur pour renforcer sa propre crédibilité », avertit l'agence de sécurité du gouvernement américain US-CERT.

Un exemple de la facilité avec laquelle les gens peuvent tomber dans le piège de l'ingénierie sociale a été révélé récemment par les organisateurs de la conférence InfoSecurity Europe. Des experts ont convaincu 90 pour cent des employés arrêtés dans la gare de Waterloo à

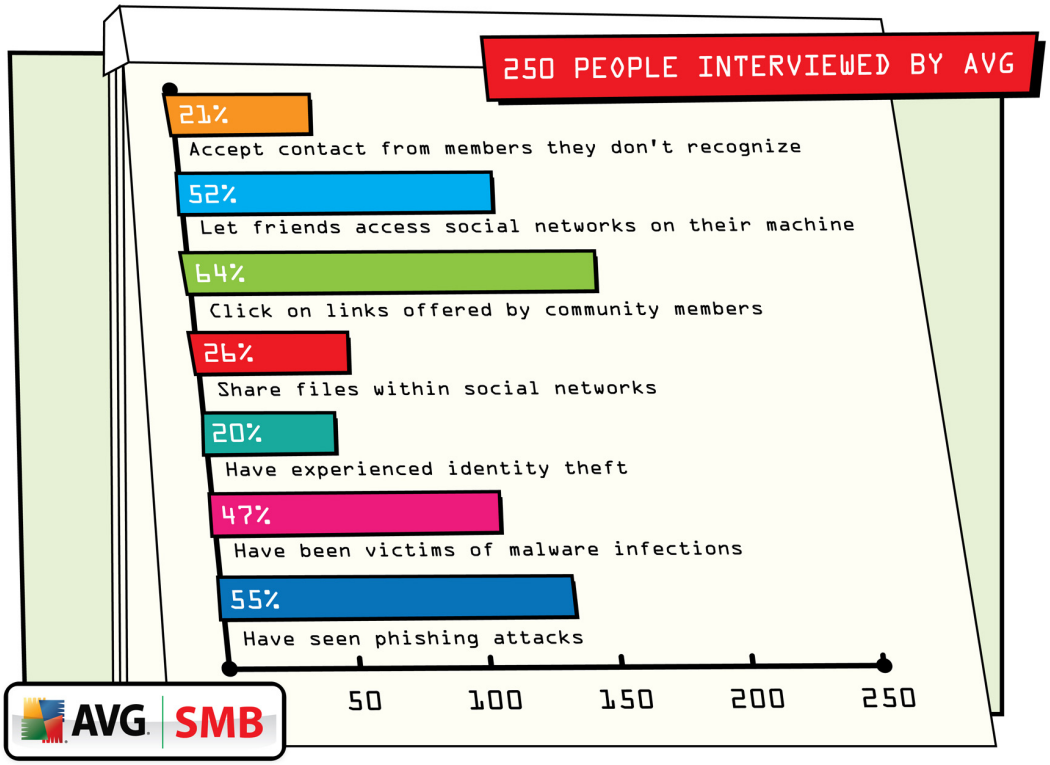
Londres de leur révéler leur mot de passe en échange d'un stylo gratuit. Quelques employés plus soupçonneux ont refusé dans un premier temps, mais finalement révélé suffisamment d'informations pour permettre aux experts de deviner leur mot de passe avec précision.

Kevin Mitnick, l'un des pirates les plus célèbres de tous les temps, a reconnu que l'ingénierie sociale était une partie essentielle de son approche. « Lorsqu'une personne moyenne imagine un pirate informatique, elle pense généralement à un petit génie de l'informatique, solitaire et introverti, dont le meilleur ami est son ordinateur et qui a du mal à tenir une conversation autrement que par messagerie instantanée », explique Mitnick dans son ouvrage intitulé L'art de la supercherie. « Pourtant, l'ingénieur social, qui possède souvent des dons pour la piraterie informatique, dispose également de grandes qualités humaines – une aptitude bien développée à utiliser et manipuler les gens qui lui permet de les persuader de lui confier des informations incroyables. »

Méfiez-vous du hameçonnage

Toutefois, l'ingénierie sociale n'a pas à être réalisée en personne ni par téléphone. L'une des techniques d'ingénierie sociale les plus populaires est le hameçonnage, qui consiste pour les criminels à bombarder les utilisateurs d'ordinateurs d'e-mails provenant prétendument de leur banque ou d'un autre organisme de confiance où des informations précieuses sont protégées par des mots de passe. Les destinataires sont invités à répondre à ce message en cliquant sur un lien qui semble légitime et en saisissant leurs identifiants de connexion. « Un pirate peut envoyer un e-mail qui semble provenir d'une société de cartes de crédit ou d'un établissement financier réputé et qui demande des informations concernant le compte, laissant souvent entendre qu'un problème est survenu », explique le site Web du CERT américain. « Lorsque les utilisateurs fournissent les informations demandées, les pirates peuvent les utiliser pour accéder aux comptes ».

Une enquête récente réalisée par AVG a révélé qu'environ 55 pour cent des 250 utilisateurs interrogés avaient reçu des e-mails de hameçonnage. L'enquête s'est notamment intéressée à la manière dont l'utilisation croissante de sites de réseaux sociaux tels que Facebook, Twitter et MySpace contribuait au développement du hameçonnage et d'autres menaces pour la sécurité.

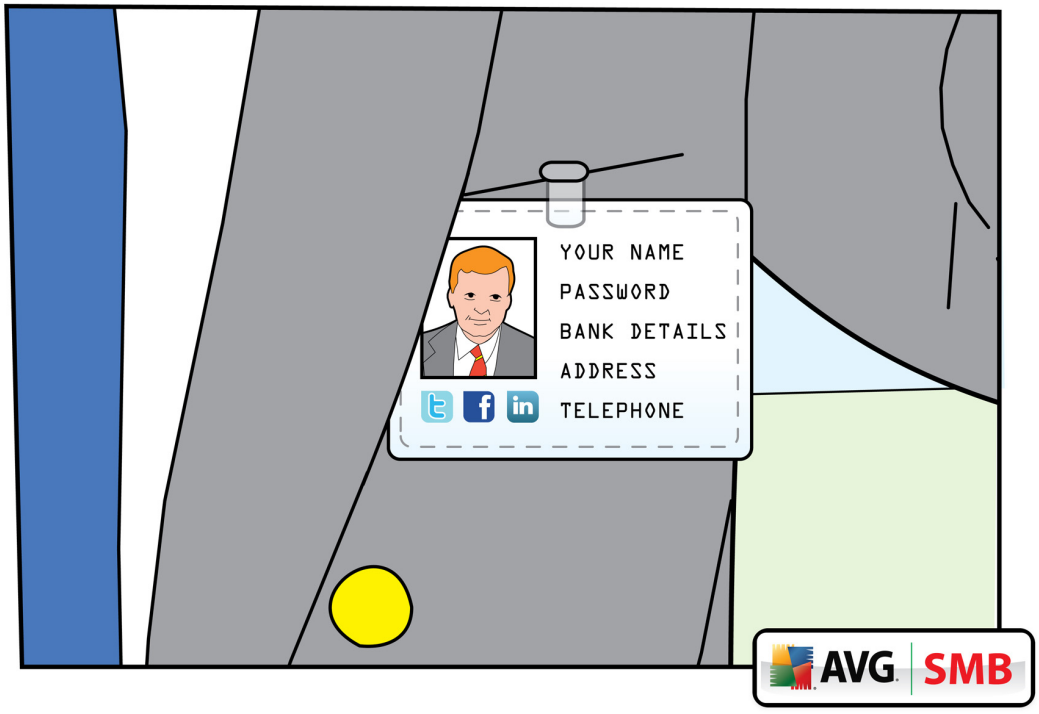


L'émergence des sites de réseaux sociaux a abouti à un mélange de techniques de piratage

de type programmation et d'ingénierie sociale, une menace identifiée par AVG dès 2007. « Le secteur des antivirus traverse une période de transition depuis deux ou trois ans et les logiciels malveillants se sont transformés, passant de simples virus à des piratages de sites web malveillants et complexes qui associent les exploits et l'ingénierie sociale pour inciter les utilisateurs ignorants à divulguer leurs données », explique le stratège de la sécurité mondiale d'AVG Technologies, Larry Bridwell.

La formation est indispensable
Lorsqu'il s'agit de se protéger contre les attaques par ingénierie sociale, les technologies comme celle d'AVG ont un rôle important à jouer. Toutefois, les experts reconnaissent que la formation du personnel est indispensable. « Un personnel bien formé est la principale ligne de défense contre les menaces en ligne dans l'entreprise », proclame la campagne GetSafeOnline soutenue par le gouvernement britannique ; le CERT américain est plus précis dans ses conseils : « Méfiez-vous des appels téléphoniques, des visites ou des e-mails non sollicités provenant de personnes qui demandent des informations à propos des employés ou d'autres renseignements internes de l'entreprise. Si un inconnu prétend appartenir à une organisation légitime, essayez de vérifier son identité directement auprès de l'entreprise ».

La meilleure stratégie pour les entreprises consiste à faire comprendre à leurs employés que la divulgation de toute information à une personne dont les motivations sont suspectes ou inconnues n'est pas une bonne idée. Cette attitude « paranoïaque » devrait être enseignée aux nouveaux employés dès leur arrivée. Ces derniers sont en effet les plus vulnérables aux technologies d'ingénierie sociale, selon Kevin Mitnick. « Les nouveaux employés sont une cible idéale pour les pirates. Ils ne connaissent pas encore beaucoup de monde et ne sont pas familiarisés avec les procédures et les interdits de l'entreprise. De plus, ils s'efforcent de faire bonne impression et sont impatients de montrer à quel point ils peuvent être coopératifs et rapides à répondre », explique-t-il.



Naturellement, il est toujours recommandé de renforcer la formation par une protection. Les entreprises devraient donc s'assurer qu'elles ont installé des logiciels de sécurité à jour. AVG 10.0 intègre une technologie qui permet de déterminer rapidement et avec précision si une page Web héberge ou non une attaque par hameçonnage.

Les criminels réussiront toujours à trouver les failles de toute armure de sécurité du système informatique d'une entreprise, mais en s'attachant aux personnes autant qu'aux ordinateurs, les entreprises peuvent compliquer considérablement la tâche des pirates.

AVG SMB group :
bit.ly/AVGSMB

Devenez fan d'AVG :
facebook.com/avgfree

Lisez nos blogs :
blogs.avg.com

Suivez-nous sur :
twitter.com/
officialAVGnews

Devenez un affilié AVG :
avg.com/gb-en/
affiliate

Regardez notre chaîne :
youtube.com/user/
officialAVG

AVG Technologies France
1, Place de la Chapelle
64600 Anglet
France
www.avg.fr

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
République Tchèque
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
États-Unis
www.avg.com/us-en/
homepage

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Royaume-Uni
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Allemagne
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosie, Chypre
www.avg.com

AVG AU TRAVAIL