KASPERSKY lab

SENSIBILISEZ VOS COLLABORATEURS À LA SÉCURITÉ INFORMATIQUE

Livre blanc

www.kaspersky.fr

SOMMAIRE

INTRODUCTION

Les responsables informatiques sont conscients des risques qui pèsent sur leur entreprise et s'équipent de plus en plus en conséquence. L'erreur humaine est moins appréhendée aujourd'hui par manque de recul ou par manque de solutions à disposition.

Découvrez dans ce livre blanc les différentes techniques utilisées par les cybercriminels pour tenter d'infiltrer les entreprises en utilisant les faiblesses de leurs salariés, mais également les conseils de nos experts pour mettre en place des méthodes simples au sein de votre entreprise afin d'anticiper ces nouveaux défis.

TECHNIQUES UTILISÉES PAR LES CYBERCRIMINELS ET CHIFFRES CLÉS

Les différents visages du phishing

Le phishing est la méthode préférée des cybercriminels pour infecter les ordinateurs des utilisateurs. Les employés des entreprises sont particulièrement vulnérables ; ils sont régulièrement pris pour cible car ils représentent un point d'entrée pour accéder à des données sensibles.

En pratique, l'utilisateur reçoit un email avec un contenu qui en apparence émane d'une institution telle qu'une banque, les impôts, la CAF ou encore un fournisseur d'accès à Internet. L'utilisateur est invité à effectuer une opération de type changement de mot de passe ou encore activation de compte mais le site web vers lequel il est dirigé est en fait une copie frauduleuse du site institutionnel.
L'employé néophyte en informatique ne sait pas faire la différence entre un email frauduleux et une communication officielle et communiquera volontairement les informations requises.

Sur le 1er trimestre de l'année 2015 nos experts ont constaté une augmentation d'1 million de déclenchements d'alertes de phishing par rapport au trimestre précédent (parmi nos utilisateurs protégés).

Les banques, les boutiques en ligne et les systèmes de paiement restent les organisations les plus ciblées par ce type d'attaque.

L'ingénierie sociale

L'ingénierie sociale est un type d'atteinte à la sécurité que les escrocs utilisent pour inciter des personnes à leur communiquer des données permettant d'accéder à des informations sensibles.
Les auteurs d'attaques d'ingénierie sociale ont le même objectif que les pirates, mais leur action consiste à tromper leurs victimes plutôt qu'à pénétrer les réseaux.
Parfois, les escrocs parviennent à obtenir les informations recherchées en les demandant tout simplement à leurs victimes.

Macros et scripts malveillants intégrés en tant qu'objet

Certains messages malveillants contiennent une pièce jointe au format .doc ou .xls dont l'ouverture lance l'exécution d'un script VBA. Ce script télécharge et installe dans le système d'autres malwares, comme des chevaux de Troie bancaires ou encore des cryptomalwares.

Nous avons également intercepté des messages dans lesquels le script était présenté sous la forme d'un objet. Les auteurs d'un de ces messages signalaient au destinataire qu'il devait s'acquitter d'une dette dans le courant de la semaine, sans quoi il s'exposait à une poursuite devant les tribunaux, ce qui occasionnerait des frais supplémentaires.
Le fichier joint était lui aussi au format Word, mais le script VBS était intégré en tant qu'objet. Afin de tromper l'utilisateur, le script apparaissait sous la forme d'un fichier Excel. Les escrocs avaient tout simplement utilisé l'icône de cette application et ajouté ".xls" au nom du fichier.

Plusieurs failles humaines peuvent être exploitées avec les différentes méthodes de phishing :

- *Le manque de connaissance des collaborateurs qui cliquent sans se poser de question*
- *L'ingénierie sociale, qui exploite les failles humaines afin d'obtenir des informations confidentielles*
- *La méconnaissance de l'outil informatique avec le déguisement des scripts malveillants en tant que fichier Excel familier pour l'utilisateur*
- *La peur de l'utilisateur avec des menaces de poursuites judiciaires*

Les chiffres clés du phishing :

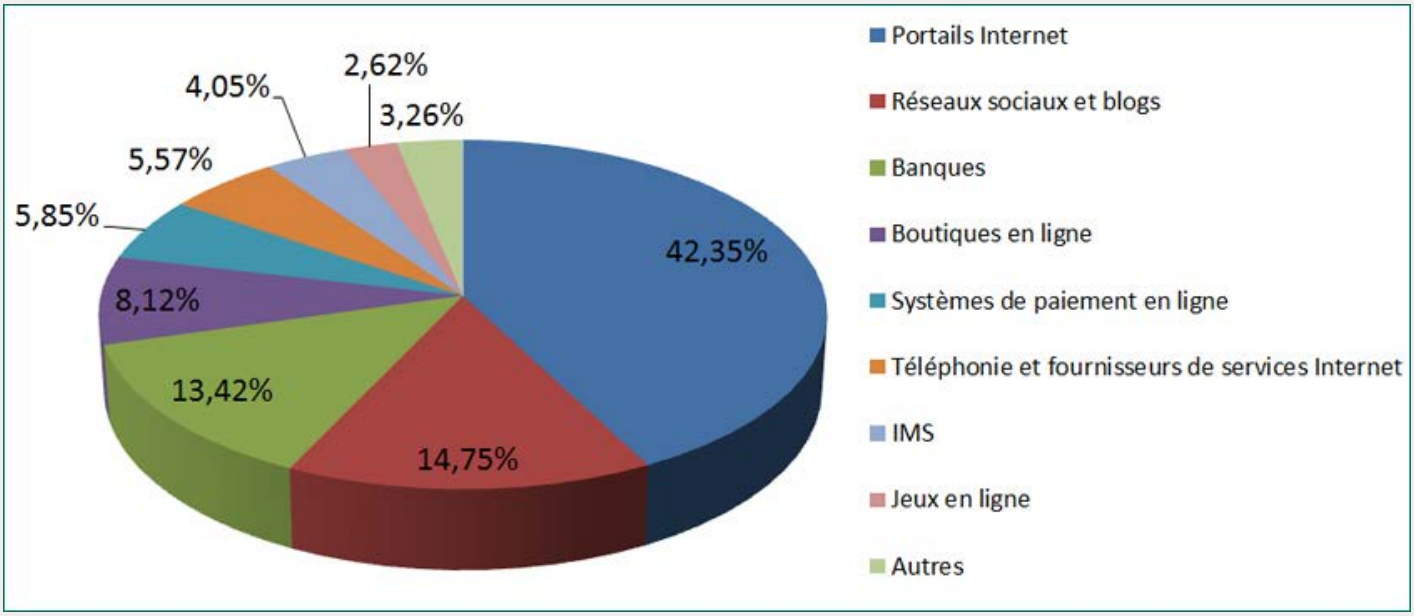
Au deuxième trimestre 2015, le système anti-phishing s'est déclenché **30 807 071 fois** sur les ordinateurs des clients de Kaspersky Lab. Au cours de cette période, **509 905** URL de phishing ont été ajoutées à la base de données de Kaspersky Lab.

Top 10 des pays en fonction du pourcentage d'utilisateurs attaqués :

	Pays	% d'utilisateurs
1	Brésil	9,74%
2	Inde	8,3%
3	Chine	7,23%
4	Russie	6,78%
5	France	6,54%
6	Japon	5,93%
7	Malaisie	5,92%
8	Pologne	5,81%
9	Kazakhstan	5,79%
10	UAE	5,75%

Au deuxième trimestre 2015, la catégorie des portails Internet populaires arrive en première position dans le classement des entreprises attaquées par des hackers.

Répartition des entreprises touchées par des attaques de phishing par secteur d'activité, deuxième trimestre 2015



Source : Viruslist Kaspersky Lab
IMS : Instant Messaging Services (Services de Messagerie Instantanée)

Infections via les périphériques amovibles

Souvent, l'employé connecte ses périphériques personnels sur diverses machines en dehors de l'entreprise, ces ordinateurs pouvant être infectés par des codes malveillants développés pour se propager automatiquement sur tous nouveaux périphériques amovibles connectés.
Lors de la connexion du périphérique infecté sur le réseau de l'entreprise, le malware infecte automatiquement la machine hôte et a ensuite la possibilité de se propager sur les autres machines.

Le virus Stuxnet s'est initialement introduit dans des installations nucléaires iraniennes via une clé USB, avant de se propager dans des installations russes de la même manière. Des programmes malveillants ont même été détectés dans une station spatiale internationale.
Kido, autrement connu sous les noms de Conficker et Downadup est un malware qui exploitait notamment les périphériques amovibles pour se propager. Il a causé des dégâts importants en entreprise et persiste encore dans certaines d'entre elles à ce jour.

La technique de propagation repose sur la facilité avec laquelle l'utilisateur peut connecter ses périphériques d'une machine à l'autre et notamment sur des ordinateurs personnels dont les niveaux de protection antivirus et d'hygiène informatique sont souvent plus faibles qu'en entreprise.

Les chiffres clés des infections via les périphériques amovibles

Les supports amovibles tels que les clés USB et les cartes SD représentent 30% des infections par des programmes malveillants.

Près d'**1/3** des entreprises ont enregistré des cas de perte/vol de mobiles d'employés.

1/4 d'entre elles savent qu'elles ont perdu des données de ce fait.

Source : Kaspersky Lab

Le BYOD* au cœur du problème

La moitié des utilisateurs de smartphones et de tablettes interrogés se servent de leur propre appareil mobile pour le travail. Cependant, seul 1 sur 10 se préoccupe sérieusement de protéger ses informations professionnelles contre les cybercriminels.

Beaucoup d'employés de grandes ou moyennes entreprises utilisent leurs appareils mobiles personnels au travail : **36 %** des participants à l'enquête* y conservent des fichiers professionnels, et **34 %** des e-mails professionnels.

Parfois, des informations plus confidentielles peuvent elles aussi se trouver sur les mobiles des utilisateurs : **18%** y stockent les mots de passe donnant accès à leur compte de messagerie professionnelle, dont **11 %** concernent des accès réseaux ou des VPN. Or ce type d'informations représente une cible parfaite pour les cybercriminels à la recherche de secrets d'entreprise.

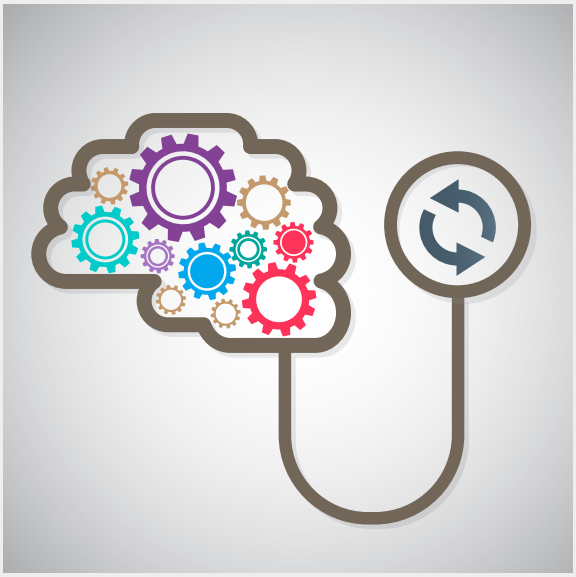
Vulnérabilités des applications

La plupart des entreprises sont maintenant équipées d'une solution d'automatisation de l'installation des mises à jour Microsoft Windows, avec un système de type WSUS.
Cependant peu d'entreprises disposent de solutions de mises à jour des applications tierces telles qu'Adobe Reader, Flash Player, Java ou encore des navigateurs tiers. Or des failles de sécurité sont fréquemment découvertes dans ces applications et les vulnérabilités sont exploitées par des codes malveillants.
Lorsque l'utilisateur dispose de tous les privilèges sur son système, ce qui en soit est déjà un problème de sécurité, on ne peut pas compter sur lui pour mettre à jour ces applications tierces.

L'inaction de l'utilisateur face aux mises à jour proposées est exploitée comme faiblesse pour que les auteurs de codes malveillants parviennent à leur objectif.

*Source : enquête 2015 réalisée par Kaspersky Lab et B2B International

Le casse-tête de la mise à jour des logiciels et des applications



Le manque de mises à jour des logiciels et le fait de ne pas patcher augmentent le risque de failles de sécurité. La plupart des malwares attaquent les vulnérabilités des applications.
Les collaborateurs ignorent souvent ou choisissent 'rappelez-moi plus tard' lorsqu'une demande de mise à jour apparait.
Il est par ailleurs complexe de contrôler les logiciels non désirables ou potentiellement dangereux installés par les salariés de l'entreprise.

Les pirates profitent du fait que les utilisateurs ne désinstallent pas les applications qui ne sont plus supportées, donc plus mises à jour mais qui fonctionnent toujours. De nombreux utilisateurs installent en effet une application, puis l'oublient*.

Les chiffres de la cybercriminalité liés aux vulnérabilités des logiciels

Plus de **14,1** millions d'attaques utilisent Java

En 2013, les vulnérabilités que contenait Oracle Java® ont été exploitées dans plus de **90 %** de l'ensemble des cyberattaques.
Les spécialistes en sécurité informatique ont rapporté plus de 160 vulnérabilités auprès d'Oracle.
En 2013, Kaspersky Lab a détecté plus de **14,1 millions** d'attaques qui utilisaient Java.
Les composants de Windows®, le système AndroidTM et le logiciel Adobe Acrobat Reader® comportent le plus grand nombre de vulnérabilités encore exploitées.

D'après une enquête réalisée en 2014 sur les risques informatiques au niveau mondial, **49%** des personnes interrogées ne procèdent pas régulièrement à l'installation des correctifs ou à la mise à jour des logiciels. **58%** des entreprises n'ont pas pleinement mis en œuvre un contrôle des applications.

Sources : Globat IT Risk survey 2014 / Kaspersky Lab, rapport de vulnérablités 2013
*Kasper Lindgaard, dirigant de Secunia – viruslist

Qualité des mots de passe

Les techniques des pirates

Les pirates utilisent des dictionnaires spéciaux qui reprennent des listes de mots qui pourraient être des mots de passe. Le hash est obtenu pour chacun de ceux-ci, puis comparé à la valeur du hash dans la base de données volée. Cette méthode requiert du temps et des processeurs puissants.

Afin de gagner du temps, les pirates utilisent des programmes spéciaux qui intègrent de grandes bases de données de mots de passe volées en différents endroits et dont les hashs ont déjà été interprétés. Ces bases sont enrichies chaque jour et après chaque attaque et dans la mesure où l'utilisateur fait preuve de paresse au moment de trouver des mots de passe très robustes et difficiles à mémoriser, le travail des pirates est considérablement simplifié.

Les mauvaises pratiques des utilisateurs

Il est fréquent qu'un utilisateur définisse des mots de passe identiques sur différents périphériques et services tels que le code PIN du smartphone, la carte bleue, la messagerie ou encore les réseaux sociaux.
Cette pratique est typique de mauvaises habitudes en matière de sécurité. Si un seul des comptes personnels est piraté, cette intrusion peut ouvrir la porte à une perte conséquente de données.

L'utilisation de mots de passe simples combinée au risque de vols de la base de données des comptes utilisateurs sur un site web sur lequel l'utilisateur est enregistré augmente grandement le risque de compromission des données.

66% des personnnes utilisent des mots de passe faciles à deviner

Les chiffres liés à la création de mots de passe

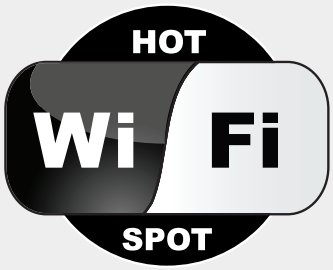
59% des individus ne stockent pas leurs mots de passe de manière sécurisée. **66%** des personnes utilisent des mots de passe faciles à deviner. **20%** utilisent le même mot de passe pour tous leurs comptes.

Source : sondage Facebook auprès des fans de Kaspersky Lab à travers le monde (33 pays et régions)-étude conduite pas O+K Research (11 000 participants)

Les réseaux WIFI publics

Le WiFi gratuit est un point chaud pour les criminels

Les escrocs peuvent pirater les connexions WiFi à accès ouvert et espionner vos activités en ligne.
Si vous ne prenez pas des précautions en matière de sécurité, les criminels peuvent voir vos noms d'utilisateurs, mots de passe, courriels et d'autres informations confidentielles.



Les hotspots WiFi sont partout

Une connectivité gratuite et pratique peut être tentante.
De nombreux employés sont équipés de périphériques mobiles tels que des smartphones ou des tablettes, depuis lesquelles ils consultent leur messagerie et échangent des données personnelles ou professionnelles.

Plusieurs dangers guettent les utilisateurs :

1. *Avec la mise à disposition de WiFi gratuit dans les lieux publics, les employés sont tentés d'envoyer des emails professionnels et de partager des informations sensibles.*
2. *La valeur de ces périphériques en fait un objet recherché et donc parfois volé, il arrive aussi que l'employé égare son matériel. Cela peut aussi engendrer de la perte d'informations confidentielles.*
3. *Le nombre de codes malveillants qui ciblent ces périphériques augmente avec la puissance et les usages multiples (consultation des comptes bancaires, envoi d'appels / SMS, etc.)*

47% seulement des utilisateurs se servent des fonctions de sécurité intégrées

Chiffres clés liés aux réseaux WIFI publics

34% des utilisateurs de wifi public ne prennent aucune mesure spécifique pour se protéger.
A peine **26 %** d'entre eux adaptent leurs activités en ligne lorsqu'ils passent par un réseau Wi-Fi public non sécurisé, et ce, en dépit du fait que des pirates peuvent facilement intercepter leurs données et leurs mots de passe. Seule la moitié des utilisateurs (**47 %**) se servent des fonctions de sécurité intégrées à l'appareil, telles que le blocage ou la localisation à distance.

Source : enquête réalisée par Kaspersky Lab et B2B International 2015

Les médias sociaux

Au cours d'une journée de travail, les employés peuvent fréquenter les réseaux sociaux, lors de leurs pauses par exemple. Entourés de leurs amis virtuels, ces derniers ont tendance à se sentir plus en confiance et à baisser leur garde, ce qui les amène à cliquer sur des liens qui renvoient vers des sites potentiellement dangereux.
Ainsi les réseaux sociaux sont souvent la cible de phishing car les employés y sont plus enclins à communiquer leurs données personnelles. Or, sur Internet, il est difficile de savoir si une personne est bien qui elle prétend être.

Les criminels peuvent par exemple tromper leurs victimes pour :

- Leur faire révéler des informations sensibles à propos de leur employeur
- Collecter des noms et des adresses électroniques afin d'envoyer des emails de phishing
- Leur faire installer un virus ou un logiciel espion
- Utiliser des informations pour pénétrer sur le réseau de leur entreprise

La diminution de la vigilance des utilisateurs sur les médias sociaux augmente les risques d'infection.

16% des organisations victimes de phishing en 2015 étaient des réseaux sociaux et des blogs.

L'usage des médias sociaux en chiffres

Les 3 principaux sites de médias sociaux visés par des attaques de phishing sont :
Yahoo ! **14.17%**
Facebook **9,51%**
Google **6.8%**

*Source : Bulletin Kaspersky Lab sur la sécurité. Spam en 2015. Les chiffres reposent sur les déclenchements du module heuristique du système Anti-Phishing sur les ordinateurs des utilisateurs des solutions Kaspersky Lab.

LES CONSEILS DE NOS EXPERTS POUR PROTÉGER VOTRE ENTREPRISE

Quelques conseils simples à mettre en place

1. Installez une solution de sécurité fiable et utilisez toutes ses fonctionnalités, notamment la recherche de vulnérabilités, le déploiement automatique des patchs et la détection rapide des virus.

2. Protégez les employés partout où ils travaillent. Avec le développement du travail mobile, appliquer des mesures de sécurité au seul matériel présent au bureau n'est plus suffisant.

3. Rédigez de façon claire et précise une politique de sécurité interne et communiquez-la largement (mails, réunions d'information).

4. Éliminez toute situation pouvant laisser la place aux comportements à risque : interdisez les applications non répertoriées (bloquer par défaut les applications inconnues).

5. Sensibilisez vos collaborateurs au fait qu'ils travaillent pour une entreprise dont les données et les informations ont beaucoup de valeur sur le marché noir de la cybercriminalité par la communication et la formation.

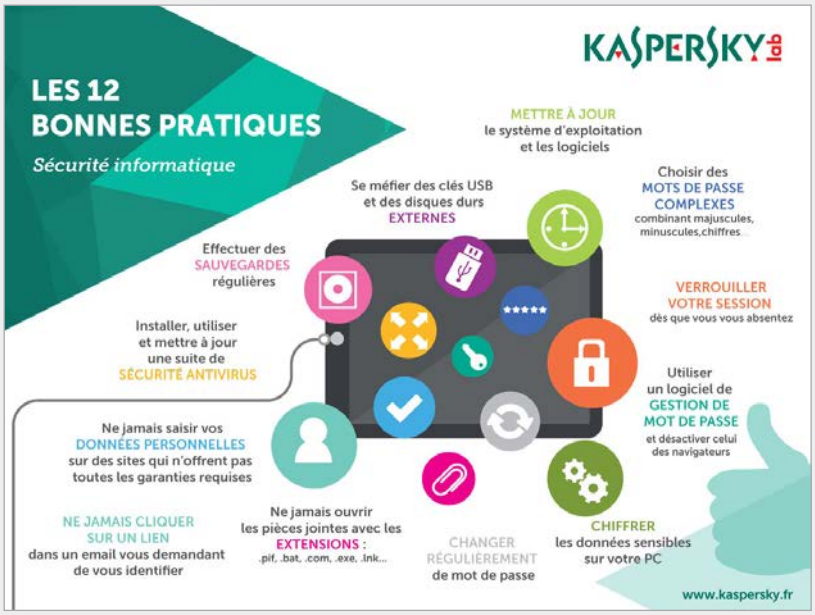
6. Réalisez des simulations d'attaques de phishing pour tester la réactivité de vos collaborateurs à ces types d'attaques.

7. N'affichez pas la liste de tous les employés sur le site Web de votre entreprise.

La formation des collaborateurs, un défi essentiel

Kaspersky Lab met à votre disposition un certain nombre d'outils pour vous aider dans votre démarche de sensibilisation de vos collaborateurs.

Découvrez notre documentation sur les dangers du phishing



Les 12 bonnes pratiques à diffuser sous format PDF

Téléchargez notre infographie sur l'utilisation des mots de passe

Une plateforme de formation en ligne pour former les salariés de votre entreprise à la sécurité informatique de façon simple et ludique :

- Formation complète de vos collaborateurs

- 17 modules de formation sous la forme de jeux et de Quiz (sur le phishing, la création de mots de passe robustes, l'utilisation des médias sociaux…)
- Simulation de campagnes de phishing, pour tester leurs réactions

- Espace administrateur performant

- Suivi des performances et de la progression des utilisateurs
- Production de rapports détaillés

Découvrez la plateforme en moins de 4 minutes

Téléchargez la brochure sur la plateforme de E-learning de Kaspersky Lab


KASPERSKY

SENSIBILISATION
DE VOS COLLABORATEURS
À LA SÉCURITÉ INFORMATIQUE

PLATEFORME DE 'E-LEARNING'

Kaspersky Online Skills Training Platform

Les menaces informatiques se multiplient et les utilisateurs sont finalement peu armés pour y faire face. Une seule erreur de leur part peut compromettre l'entreprise, lui faire perdre de l'argent ou sa réputation.
Votre challenge en tant qu'acteur de la sécurité de votre entreprise est de faire de l'utilisateur un partenaire de la sécurité.

Pour vous accompagner dans cette démarche, nous avons mis au point une plateforme de « E-learning » interactive et ludique, composée de jeux et de quiz, qui vous permettront de mesurer le niveau de connaissance des salariés de votre entreprise en matière de sécurité informatique et de les faire progresser.

Fonctionnement :

- Un accès à la plateforme utilisateur : 17 modules de formation (jeux et quiz) en ligne
- Un accès à la plateforme d'administration pour suivre les performances de vos collaborateurs et tester leurs réactions

LES ATOUTS DU JEU

- Permet de faire progresser ses collaborateurs sur les problématiques de sécurité et de leur fait prendre conscience des enjeux.
- S'adresse à tous les profils de l'entreprise.
- Ludique et progressif.
- Flexibilité de la formation en ligne : des objectifs sont donnés aux collaborateurs sur une période donnée. Ils gèrent leurs temps de connexion au cours de leurs journées de travail.
- Pas de limite de nombre de joueurs.


Twitter.com/
kasperskyfrance


Facebook.com/
kasperskylabfrance


Youtube.com/
user/KasperskyFrance

Kaspersky Lab France
www.kaspersky.fr

Tout sur la sécurié internet:
www.securelist.fr

Pour toute demande d'information :
Information-services@kaspersky.fr