G Data

Whitepaper 12/2009

Shopping en ligne sécurisé : acheter correctement des cadeaux de Noël sur Internet

Sabrina Berkenkopf & Ralf Benzmüller
G Data Security Labs

Whitepaper_12_2009_FR

Go safe. **Go safer. G Data.**

Contenu

Le shopping en ligne en plein essor

La popularité du commerce en ligne n'a cessé d'augmenter au cours des dernières années au sein de l'UE. En 2008, presque un tiers (32 %) des Européens âgés de 16 à 74 ans utilisaient Internet afin de commander des produits et services à usage personnel. Ce chiffre décrit une augmentation de 12 % en l'espace de quatre ans (source : Eurostat).

En France, les achats en ligne explosent. Ainsi, selon la fevad (fédération du e-commerce et de la vente à distance, www.fevad.com) et l'institut Médiamétrie/NetRatings, 70 % des internautes ont l'intention d'acheter leurs cadeaux de noël en ligne en cette fin d'année. Un engouement qui se concrétise dans les chiffres de vente. Toujours selon la fevad, les français devraient dépenser plus de 5 milliards d'euros sur Internet à l'occasion des fêtes, soit une progression de 25 % comparé à 2008.

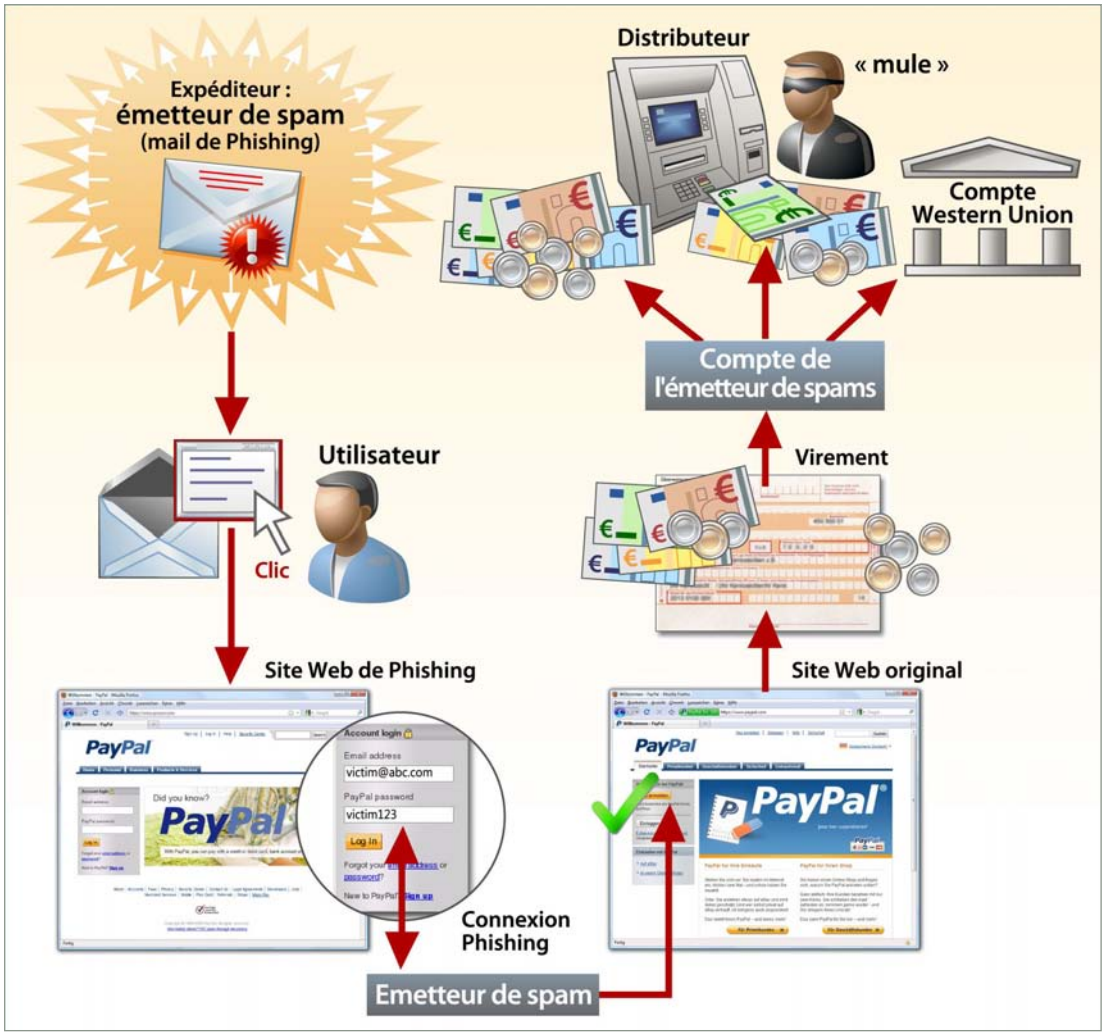
Attaque d'hameçonnage sur des données d'acheteurs

L'hameçonnage décrit l'espionnage et l'usage de données personnelles en tout genre par un cybercriminel. Une pratique qui a considérablement augmenté au cours des dernières années. La vente d'informations de cartes de crédit, de comptes bancaires en ligne et de données d'accès à des services fiduciaires, comme PayPal, est particulièrement lucrative pour les cyber-délinquants. Les cibles des cyber-délinquants sont avant tout les mots de passe et données d'accès de comptes utilisateurs, de banques en ligne, de plateformes commerciales, de réseaux sociaux ou de jeux en ligne. En Allemagne, l'institut Bitkom a publié, en collaboration avec le BKA, l'information selon laquelle 5 % des internautes de 14 ans et plus ont été victimes d'hameçonnage.

Le piège le plus fréquent pour accéder aux données de l'utilisateur est l'envoi de urriers électroniques d'hameçonnage, dont le design copie celui d'une grande entreprise. Alors qu'ils pouvaient autrefois être facilement démasqués en raison de leur orthographe incorrecte, d'erreurs de grammaire, d'inflexions manquantes et de caractères spéciaux, ils sont aujourd'hui souvent impeccables au niveau de la forme et de la langue. Banques, prestataires d'expédition et éditeurs de jeux vidéo renommés servent de modèles à ces courriers électroniques.

Ill. 1 : capture d'écran d'un courrier de phishing PayPal

En pratique, la cible d'une attaque d'hameçonnage est invitée à suivre un lien et à entrer ses données d'accès au site Web. Le piège le plus courant : faire croire au destinataire que le site Web auquel il fait confiance et qui est mentionné dans le courrier électronique (eBay, PayPal ou autres) a mis à jour des directives de sécurité. L'utilisateur est alors invité à se connecter pour les accepter/s'inscrire. Dans d'autres cas, le destinataire du courrier électronique est prié de mettre à jour ses données personnelles et est là aussi dirigé vers une fausse page Internet.



Ill. 2 : schéma d'une attaque de phishing

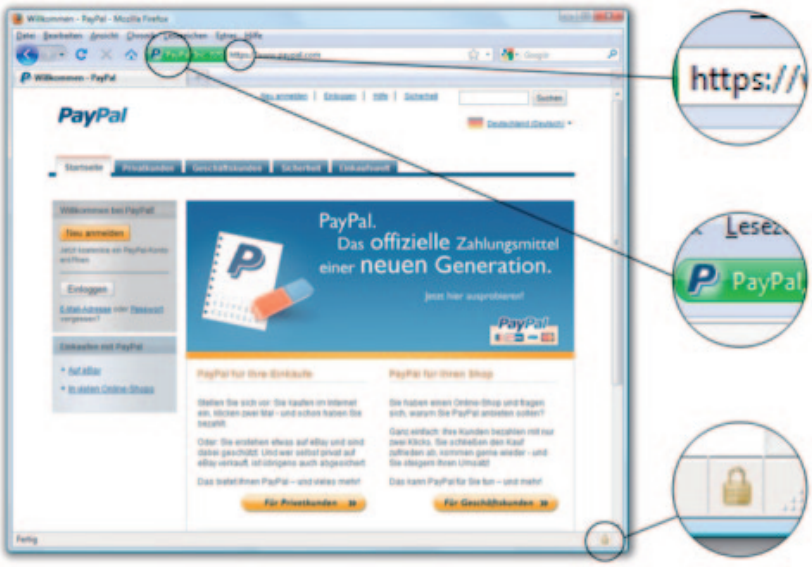
Un autre piège, critique pendant cette période de Noël, consiste à faire croire à l'utilisateur qu'il doit se connecter à une page web pour consulter l'état d'expédition de ses achats. Les sites Web frauduleux sont souvent difficilement différenciables des originaux.

Nom d'utilisateur, mot de passe, numéro de compte ou de cartes bancaires, toute donnée communiquée peut potentiellement être utilisée par le cyber-délinquant. Les informations d'accès du compte de messagerie électronique sont par exemple très recherchées : elles permettent de réinitialiser les mots de passe de nombreux comptes.

Le maillon faible dans une attaque d'hameçonnage est bien entendu l'utilisateur. Les données entrent en possession des cyber-délinquants par la saisie « volontaire» de l'utilisateur. De ce fait : les courriers électroniques d'expéditeurs inconnus doivent être traités avec méfiance. Il convient de ne cliquer sur aucun lien qui conduit à des pages d'inscription de supposés portails bancaires, eBay ou autres. Aujourd'hui, plus aucune entreprise ne communique par courrier électronique au sujet des données clients !

Caractéristiques de sécurité des sites Web et boutiques en ligne

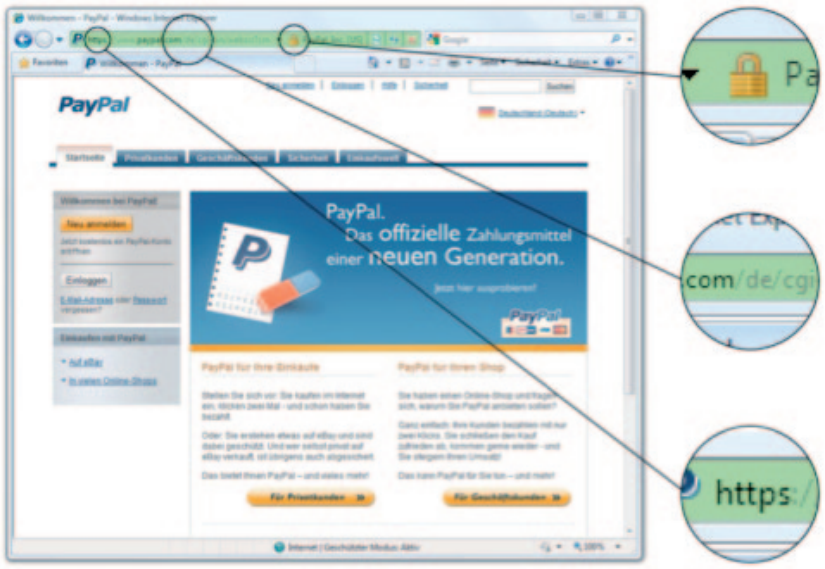
Si un Internaute est invité à visiter une page impliquant la saisie de données personnelles, il doit être attentif aux caractéristiques de sécurité suivantes : un symbole de cadenas affiché dans le navigateur et la mention https au début de l'adresse Web. Depuis peu, dans de nombreux navigateurs Internet, les sites Web chiffrés sont affichés avec une ligne d'adresse colorée en vert, ce qui aide l'identification. Ces caractéristiques de sécurité doivent non seulement être respectées sur les pages bancaires, mais également lors de paiements directs dans les boutiques en ligne en cas d'achat par carte de crédit ou par prélèvement bancaire, mais aussi lors de la connexion à des services de paiement comme PayPal. Si une boutique en ligne exige un enregistrement préalable de l'acheteur, ces données d'enregistrement personnelles doivent également être envoyées au commerçant, par une connexion sécurisée. Internet Explorer 8 affiche également le domaine de premier niveau de la page Web en lettres noires et les parties restantes en gris. Il peut ainsi être garanti d'accéder réellement à une page officielle, comme eBay, et non pas à une fausse adresse qui possède uniquement eBay comme composante de son nom à des fins de tromperie.



Ill. 3 : capture d'écran d'une page sécurisée dans Mozilla Firefox 3.5

En outre, il convient de veiller à ce que les boutiques en ligne sélectionnées soient dignes de confiance. Des prestataires mondialement connus, par exemple amazon.com, ont une réputation positive et sont établis sur le marché en ligne. Lors de la sélection d'un prestataire moins connu, les faits suivants peuvent renseigner sur son authenticité :

- Le prix proposé pour un produit est-il «dans la fourchette» ou bien étonnamment faible ?
- Les descriptifs et images du produit concordent-ils ?
- Les frais d'envoi sont-ils clairs et appropriés ?
- La boutique en ligne possède-t-elle des conditions générales de vente ?
- Suis-je d'accord avec les informations et conditions mentionnées dans les conditions générales de vente ?
- Le site Web possède-t-il des mentions légales ?
- Puis-je trouver la boutique dans des moteurs de recherche ? Est-elle connue ?



Ill. 4 : capture d'écran d'une page sécurisée dans Internet Explorer 8

Utilisation correcte des mots de passe

Pour limiter les effets de l'hameçonnage, il convient de multiplier les mots de passe. Ainsi, le vol des informations relatives à un compte ne met pas en péril les autres comptes de l'utilisateur. Ceci introduit la problématique du bon usage des mots de passe. Pour protéger des comptes utilisateurs, l'emploi de mots de passe fortement sécurisé est conseillé. Les mots de passe tels que «admin» ou «mot de passe123» ne font pas partie de cette catégorie ! Une combinaison de 8 lettres au minimum en majuscules et en minuscules, de chiffres et de caractères spéciaux génère des mots de passe à haut niveau de sécurité, par exemple Hb1&opGT58. Cette suite de caractères est un mot de passe sûr mais difficile à retenir.

Pour générer un mot de passe pouvant être retenu facilement, la technique des acronymes peut être utilisée :

The sound of silence de Simon & Garfunkel de 1966 = TsosdS&Gd1966

L'utilisation de la technique dite «Leetspeak» est également possible : les lettres sont remplacées par des chiffres et caractères similaires :

The sound of silence = 7h3_50und_0f_51l3nc3

Noms d'utilisateur et mots de passe ne doivent en général pas être enregistrés dans le navigateur, même si ceci paraît très pratique. Des données de connexion mémorisées et autres informations personnelles rendent l'utilisateur attaquable par un autre type de collecte de données par cheval de Troie.

Les chevaux de Troie infiltrent un programme nuisible sur l'ordinateur de l'utilisateur et y exécutent des procédures indésirables. L'une des procédures possibles consiste à collecter les données personnelles stockées sur l'ordinateur infecté et à les transmettre ensuite via Internet au cyber-délinquant.

Sécuriser l'environnement

Achats, transactions bancaires ou toute autre procédure sensible réalisée en ligne ne doivent pas être effectuées via un réseau sans fil public ou un cybercafé. Le risque de vol de données par des renifleurs est extrêmement élevé en cas de points d'accès Wi-Fi gratuitement accessibles et non sécurisés. Dans les Cybercafés, les cookies et autres informations de connexions se rapportant à l'utilisateur peuvent rester sur l'ordinateur public et être consultés par l'utilisateur suivant. En règle générale, les visiteurs d'un Cybercafé n'ont aucun contrôle sur les paramétrages de sécurité de l'ordinateur et doivent de ce fait se fier au savoir-faire en matière de sécurité de l'exploitant du cybercafé.

Une bonne pratique de l'utilisateur n'est pas le seul élément déterminant dans un comportement sécurisé. L'ordinateur joue aussi un rôle primordial lors de l'achat en ligne : l'ordinateur doit être équipé d'une solution antivirus fiable intégrant un filtre http et d'un pare-feu. Ceci permet à l'utilisateur d'être protégé contre de nombreux parasites (chevaux de Troie, virus, vers, etc.), de scanner ses e-mails pour détecter l'hameçonnage ou le spam (comme, par exemple, invitations au casino et différents produits pharmaceutiques) et de filtrer les contenus indésirables.

En outre, un filtre HTTP peut scanner en direct tout le trafic en ligne entrant et sortant et bloquer directement les menaces afin que des sites Web malveillants ne puissent pas attribuer à l'utilisateur des contenus indésirables, comme, par exemple, Gumblar, le cheval de Troie faisant fureur actuellement. Un pare-feu règle le trafic de données complet selon des règles prédéfinies et le bloque le cas échéant, afin que les auteurs d'attaque ne puissent utiliser des portes ouvertes dans l'ordinateur.

Les auteurs d'attaque misent sur les failles de sécurité dans les systèmes de leurs victimes, dues à une gestion des mises à jour négligée. Tout le système doit donc être régulièrement mis à jour : Windows bien entendu, mais aussi tous les autres programmes installés. Dans cette démarche, le navigateur doit être une priorité. Il est par nature particulièrement sensible aux attaques par Internet et offre des failles de sécurité lorsque sa version est dépassée.

En résumé :

Pour minimiser les risques du shopping en ligne G Data recommande les six mesures suivantes :

1. Utilisez une solution antivirus, un pare-feu et un filtre HTTP.
2. Actualisez toujours le logiciel de sécurité, le programme d'exploitation et les autres logiciels.
3. Soyez méfiant lors de la réception de courriers électroniques provenant d'expéditeurs inconnus – ne cliquez sur aucun lien, ne téléchargez et n'ouvrez pas de fichiers joints.
4. Entrez manuellement les adresses de sites Web avec connexion de l'utilisateur ou utilisez la fonction de signets de votre navigateur.
5. Veillez aux caractéristiques de sécurité dans la fenêtre de navigation lorsque vous achetez en ligne :
   - Le cadenas dans le navigateur
   - L'abréviation https avant l'adresse entrée
   - La ligne d'adresse en vert dans de nombreux navigateurs récents
   - L'affichage du domaine de premier niveau correct, en particulier dans Internet Explorer 8
6. Vérifiez que la boutique de votre choix dispose de conditions générales de vente, de mentions légales et de structures de coûts bien définis (par exemple, frais d'expédition et éventuellement frais supplémentaires)