

**BitDefender : Le phishing sur la messagerie instantanée, iPad et Facebook**  
**Sécurité**

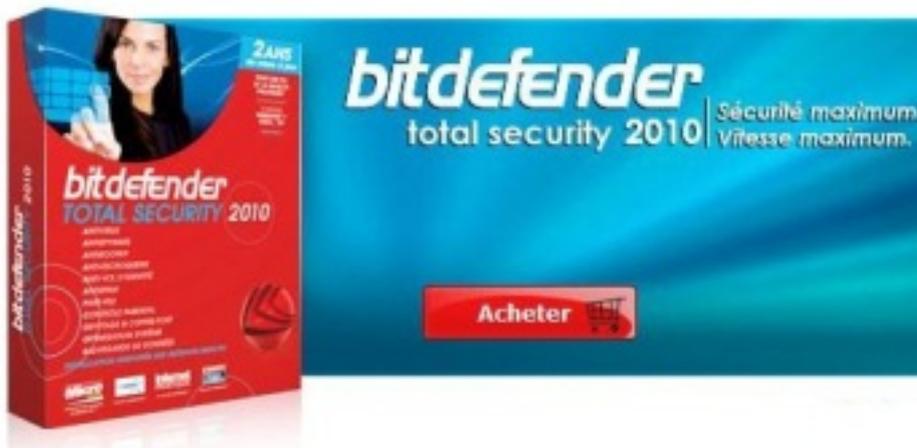
Posté par : JerryG

Publié le : 4/6/2010 15:00:00

**Le phishing s'attaque aux utilisateurs de messagerie instantanée**, en toute simplicité. Une application Internet « vient à l'aide » des utilisateurs MSN & YIM qui souhaitent savoir si leurs amis, collègues ou connaissances les ont bloqués

Il n'est pas toujours facile de gérer vos profils de réseaux sociaux lorsque ceux-ci commencent à s'accumuler et que le nombre de vos « followers » est en augmentation constante. Chaque membre d'une communauté sociale – tant au centre d'un réseau de connexions, l'une des façons de gérer ce monde chaotique d'amis et « d'amis d'amis » consiste à découvrir si nous avons été bloqués, mis en liste noire ou supprimés de la liste de nos contacts.

**Ces utilisateurs particulièrement actifs de MSN & YIM** sont la cible d'une attaque d'ingénierie sociale particulièrement bien pensée. Pour découvrir qui les a gardés dans leur liste de contacts, ils doivent simplement indiquer sur la page Internet Blocked or Not leurs identifiants de compte et les mots de passe associés.



Une fois les identifiants saisis, les utilisateurs curieux (et naïfs) ne sont plus qu'à un clic de découvrir quels « amis » les ont mis en liste noire.

La réponse, toujours la même, est confortante : aucun ami ne vous a bloqué au cours des deux derniers mois !

**Et maintenant, la charge utile :** d'une part, un nombre considérable d'identifiants de comptes (noms d'utilisateurs et mots de passe) est recueilli afin de perpétrer des actions illégales, telles que des arnaques, des attaques de spam ou des usurpations d'identité. Et ce n'est pas tout : les données volées permettent aux attaquants d'espionner des

conversations personnelles, de connecter des identifiants YIM/MSN à d'autres comptes utilisateurs et même de réinitialiser les mots de passe de services bancaires.

**D'un autre part**, au moment où les utilisateurs se réjouissent de la loyauté de leurs amis, ils sont redirigés vers une page de publicités qui leur propose tout un ensemble d'offres telles que des films, des études et des jeux gratuits en ligne. Les jeux sont en fait des salles de chat pornographiques et rien n'est gratuit.

Il semble que demander aux utilisateurs de remplir des questionnaires soit une stratégie relativement lucrative, puisqu'elle est désormais utilisée à grande échelle afin de générer des revenus à partir du trafic des sites web. Cette approche rappelle celle qui a été employée il y a deux jours dans le cadre de l'arnaque de clickjacking sur Facebook.

**Pour Rappel :**

**Une arnaque de phishing exploitant l'iPad est présente sur Facebook.** Les réseaux sociaux : particulièrement efficaces pour les fausses campagnes de marketing

Vous aimeriez obtenir un des iPads tant convoités en remplissant simplement un questionnaire ? L'offre est tentante ! Rappelez-vous cependant que lorsque quelque chose a l'air trop beau pour être vrai, c'est qu'il est généralement le cas !

**L'arnaque est extrêmement présente sur la page événements de Facebook**, où environ 2 500 personnes se sont inscrites à cet événement et sont probablement déjà victimes de cette attaque de phishing. L'identité de départ est très simple : vous vous inscrivez pour « tester » un iPad, vous obtenez le produit avec un questionnaire que vous devez compléter et renvoyer à l'entreprise. Bien évidemment, vous conservez l'appareil testé sans aucune autre obligation.

**La page de phishing**, masquée par une URL raccourcie, commence par demander des informations plutôt raisonnables telles que le prénom et l'adresse e-mail avant de passer à tout un ensemble de données dont le nom complet, l'adresse personnelle et les numéros de téléphone. Afin de ne pas éveiller de soupçons, les pirates ont ajouté des logos de médias connus, bien que ceux-ci n'aient aucun lien avec cette initiative.



Une fois ces données recueillies, le pirate demande à l'utilisateur d'accepter un dernier contrat de sécurité et d'indiquer son nom d'utilisateur et son mot de passe Facebook. Pour couronner le tout et causer plus de dommages, l'utilisateur non averti dont le compte vient d'être « volé » est invité à télécharger et à installer une application adware (une barre d'outils pour navigateur) qui modifie la page de démarrage du navigateur et le moteur de recherche par défaut, entre autres choses.

Inutile de préciser qu'une fois les données personnelles récupérées, le compte piraté et la barre d'outils installée, les utilisateurs ne recevront jamais l'iPad promis et n'entendront plus parler des attaquants.

**Cette arnaque s'inspire d'une pratique couramment utilisée par les fabricants**, qui consiste à envoyer plusieurs unités d'un produit afin de les faire tester. Cependant, recevoir des appareils destinés à être testés n'est pas donné à tous, et cette offre est généralement destinée aux blogueurs en vue et, surtout, aux sites web spécialisés. Cependant, même dans ce cas, l'éthique des journalistes préconise que le testeur retourne l'objet une fois celui-ci évalué.

Facebook a été averti et cette page d'avertissements a été supprimée.

**[Pour plus d'informations concernant les produits BitDefender.](#)**