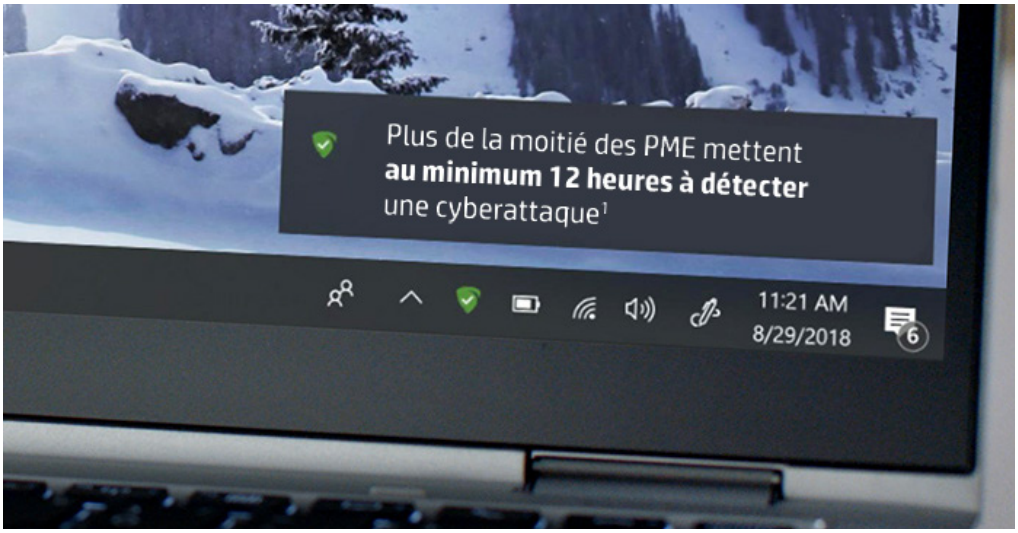
Le hameçonnage ne se cantonne désormais plus aux e-mails

En savoir plus



Un navigateur web est un portail vers un monde d'informations… et de menaces. Quelles mesures pouvez-vous donc prendre pour protéger votre entreprise ?

Les navigateurs web ont encore beaucoup à faire en termes de protection contre les attaques. Dans un sondage récent réalisé auprès de 400 DSI, 68 % d'entre eux ont déclaré que les techniques employées par les cybercriminels sont désormais si élaborées que leur personnel peine à différencier les sites sécurisés de ceux qui ne le sont pas[2]. Dans ce contexte, il n'est pas étonnant que près de 70 % des professionnels de l'informatique subissent des attaques d'hameçonnage chaque semaine, et pas seulement par e-mail[3]. Les pirates, qui ont perfectionné leurs stratagèmes, utilisent désormais les réseaux sociaux, les publicités et les fautes d'épellation de sites internet plébiscités afin de duper les employés et les inciter à révéler des renseignements personnels sensibles. À mesure que les arnaques par hameçonnage deviennent de plus en plus difficiles à discerner, les entreprises ont du mal à protéger leur personnel de ces attaques.

En dépit de la prise de conscience généralisée et de l'investissement dans des logiciels de sécurité ainsi que dans la formation des employés, le nombre de cyberattaques sur les ordinateurs portables et de bureau a augmenté de plus de 100 %[4]. Les cybercriminels arrivent encore à agir et à impacter les entreprises grâce à un faible niveau de sécurité qui joue en leur faveur. Protéger des données requiert d'innombrables efforts, mais il suffit qu'un employé clique sur un lien malveillant pour nuire à toute votre entreprise.

Les cyberattaques sur les réseaux sociaux contribuent largement à ce problème. Les plateformes telles que Facebook et Twitter sont les terrains de chasse de prédilection des cybercriminels. Elles sont non seulement conçues pour promouvoir l'implication et la communication, mais elles sont aussi simples d'utilisation et économiques en termes d'exploitation. Il est extrêmement facile d'ouvrir des comptes frauduleux et d'envoyer des messages malveillants contenant des liens, visant à récupérer des données ou encore conduisant vers des pages de renvoi qui ouvrent des fenêtres pop-up peu fiables.

La plupart de ces activités en ligne se basent sur des techniques d'hameçonnage qui, par le passé, se cantonnaient seulement aux e-mails. Les réseaux sociaux facilitent l'établissement de liens entre les personnes, et il est malheureusement incroyablement facile d'inventer un personnage crédible qui suivra les utilisateurs authentiques sur les plateformes.

Pour la majorité des entreprises victimes d'attaques d'hameçonnage, les conséquences sont préjudiciables pour son activité et sont de longue durée. Elles peuvent non seulement se solder par une baisse de la productivité du personnel et la perte des données client, mais aussi par la perte des clients eux-mêmes. Une quelconque brèche de sécurité peut fortement miner la confiance de vos clients dans votre entreprise : à leurs yeux, vous n'êtes plus un détenteur de renseignements fiable. Bien que la plupart du temps le tort puisse être réparé, les dommages sont permanents.

Le hameçonnage ne se cantonne désormais plus aux e-mails

Au quatrième trimestre de l'année 2017, les attaques d'hameçonnage sur les réseaux sociaux ont augmenté de 500 %, avec des stratagèmes consistant à faire passer des comptes frauduleux pour le service client de grandes marques[5]. Cette tendance a été baptisée appâtage, car les pirates envoient l'appât et attendent que les utilisateurs viennent à eux. Ces attaques convaincantes, qui reposent sur l'utilisation de la même stratégie de marque et d'un nom de compte semblant authentique, bernent des millions de personnes qui font confiance aux réseaux sociaux. Ensuite, dès qu'un utilisateur mord à l'appât, le compte frauduleux lui envoie un lien vers un site d'hameçonnage en lui demandant de se connecter, ce qui permet au pirate d'accomplir sa mission et de récupérer ses données personnelles.

L'une des façons d'empêcher que vos employés ne se fassent duper par des tentatives d'hameçonnage sur les réseaux sociaux est de promouvoir un changement de comportement au travail. Votre personnel évitera ainsi de commettre de simples erreurs qui pourraient avoir des conséquences dévastatrices pour votre entreprise :

1. Limiter les interactions aux utilisateurs fiables
2. Ne pas cliquer sur les liens fournis par des sources non vérifiées
3. Ne jamais télécharger de pièces jointes sur les réseaux sociaux
4. Établir une authentification à deux facteurs sur tous les comptes de réseaux sociaux et appareils, car cette mesure entrave le piratage
5. Fournir une formation supplémentaire aux employés ayant des privilèges d'accès élevés ou dont le poste revêt un caractère social

La technologie que vous utilisez pour rester protégé sur internet est un autre aspect fondamental à prendre en compte pour l'élaboration de votre plan de sécurité. La gamme HP Elite propose par exemple une série d'ordinateurs portables, PC de bureau et postes de travail conçus dès le départ dans une optique de sécurité.

L'un de ces paramètres de sécurité, disponible sur une sélection d'appareils portables et postes de travail HP Elite, est HP Sure Click[6], lequel révolutionne la navigation sécurisée. Au lieu de se contenter de signaler aux utilisateurs les sites dangereux qu'il faut éviter, il empêche les maliciels, les rançongiciels et les virus de contaminer les autres onglets et le système en général. Lorsqu'un utilisateur lance une session de navigation, chaque site consulté déclenche HP Sure Click. Par exemple, chaque fois qu'un site est consulté, HP Sure Click crée une session de navigation isolée, basée sur le matériel informatique, qui élimine la capacité d'un site à contaminer les autres onglets ou le système.

HP Sure Click protège même les utilisateurs contre les maliciels cachés dans les fichiers Office et PDF. Imaginons que vos employés reçoivent un PDF infecté par e-mail : cette solution leur permet d'ouvrir le document en toute sécurité puisque HP Sure Click isole le fichier dans une micromachine virtuelle et évite ainsi la propagation de l'infection en dehors du fichier. Grâce à cette solution de sécurité intégrée à votre flotte de PC, vous n'aurez plus à vous inquiéter des menaces en ligne dans l'optique de disposer d'une meilleure gestion du service informatique.

Il semble souvent trop fastidieux pour les entreprises de changer leur stratégie en matière de sécurité tout en se procurant des appareils de pointe, comme les HP EliteBook x360, avec la 8e génération de processeurs Intel® Core™ i7 en option. C'est là qu'une solution comme HP Device as a Service (DaaS)[7] entre en jeu. Il s'agit d'un modèle de consommation pour ordinateur qui simplifie la façon dont les organisations commerciales fournissent à leur personnel le bon matériel et les bons accessoires, gèrent les divers appareils multi-OS, et obtiennent des services dotés d'un cycle de vie plus long. HP DaaS propose des forfaits simples et flexibles, à un prix fixe par appareil, qui permettent à votre entreprise de fonctionner efficacement, sans accrocs.

En fin de compte, une équipe bien formée et des appareils qui optimisent la sécurité vous permettront de combattre le cybercrime sur les réseaux sociaux, l'une des plus grandes menaces qui existe sur la toile. Les choses ne feront qu'aller de mal en pis, vous avez donc tout intérêt à renforcer vos défenses dès maintenant.

Découvrez les avantages des solutions de sécurité HP pour votre entreprise.

Sources :

1. Recherches menées par Osterman, commanditées par Malwarebytes : «Second Annual State of Ransomware Report: US Survey Results », juillet 2017
2. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
3. http://www8.hp.com/us/en/hp-news/press-release.html?id=1763561#.WLTLYjsrI2y
4. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar

6. HP Sure Click est disponible sur la majorité des PC HP et est compatible avec Microsoft® Internet Explorer, Google Chrome et Chromium™. Parmi les pièces jointes compatibles se trouvent les documents Microsoft Office (Word, Excel, PowerPoint) et les fichiers PDF en lecture seule uniquement, lorsque Microsoft Office ou Adobe Acrobat sont installés.

7. Les plans HP DaaS et/ou les composants inclus peuvent varier selon la région ou en fonction du partenaire de service HP DaaS agréé. Veuillez contacter votre représentant HP local ou votre partenaire DaaS agréé pour plus de détails dans votre région. Les services HP sont régis par les conditions générales d'utilisation HP applicables fournies ou indiquées au client lors de l'achat. Le client peut bénéficier de certains droits supplémentaires conformément aux lois locales applicables, et ces droits ne sont en aucun cas affectés par les conditions générales d'utilisation HP ou la garantie limitée HP fournie avec votre produit HP.

4AA7-317FRE, avril 2019