OUCH!

SANS SECURITY AWARENESS

Le bulletin mensuel de sensibilisation à la sécurité pour vous

Oui, vous êtes une cible

Vue d'ensemble

De nombreuses personnes pensent à tort qu'elles ne sont pas la cible d'attaques informatiques, que leurs systèmes ou leurs comptes n'ont aucune valeur. Cela ne pourrait pas être plus éloigné de la vérité. Si vous utilisez la technologie de quelque manière que ce soit, au travail ou à la maison, faites-nous confiance, vous valorisez les cybercriminels. Mais vous avez de la chance, vous disposez déjà de la meilleure défense contre ces cyberattaques: vous-même.

Pourquoi êtes-vous une cible ?

Il y a beaucoup de cyberattaquants sur Internet aujourd'hui, et ils ont tous des motivations différentes. Alors, pourquoi l'un d'entre eux voudrait-il vous attaquer? Parce que vous pirater les aident à atteindre leurs objectifs. Voici deux exemples courants de cyberattaquants et les raisons pour lesquelles ils vous ciblent.

⚠ **Cybercriminels:** Les cybercriminels cherchent à gagner le plus d'argent possible. Ce qui rend Internet si précieux pour eux, c'est qu'ils peuvent désormais facilement cibler toute la population mondiale en appuyant simplement sur un bouton. Et il y a BEAUCOUP de façons de gagner de l'argent par votre biais. Les exemples sont nombreux : voler de l'argent de votre compte bancaire ou de votre compte de retraite, créer une carte de crédit à votre nom et vous envoyer la facture, utiliser votre ordinateur pour pirater d'autres personnes ou pirater vos comptes de réseaux sociaux ou de jeux et les vendre à d'autres criminels. Comment les cybercriminels peuvent-ils gagner de l'argent « grâce » à vous : la liste est sans fin. Des centaines de milliers de ces cybercriminels se lèvent chaque matin dans le but de pirater autant de personnes que possible chaque jour, vous y compris.

☆ **Pirates informatiques ciblés:** Ce sont des cyberattaquants hautement qualifiés, travaillant souvent pour les gouvernements, des syndicats de criminels ou des concurrents vous visant au travail. Vous pensiez peut-être que votre travail n'attirerait pas beaucoup d'attention, mais vous pourriez être très surpris.

- Les informations que vous gérez au travail ont une valeur considérable pour différentes entreprises ou gouvernements.

- **Les attaquants ciblés peuvent vous cibler au travail non pas parce qu'ils veulent vous pirater, mais pour vous utiliser afin de pirater l'un de vos collègues ou un autre système.**
- **Ce type d'attaquants peut vous cibler au travail en raison des entreprises pour lesquelles vous travaillez ou avec lesquelles vous collaborez.**

Je possède un Anti-Virus, je suis donc en sécurité

Ok, alors je suis une cible, pas un problème. Je vais simplement installer un anti-virus et un pare-feu sur mon ordinateur et je serais protégé, n'est-ce pas? Eh bien malheureusement, non. Beaucoup de gens pensent que s'ils installent des outils de sécurité, ils sont en toute logique en sécurité. Malheureusement, ce n'est pas tout à fait vrai. Les cyberattaquants continuent d'évoluer et bon nombre de leurs méthodes d'attaques contournent désormais facilement les technologies de sécurité. Par exemple, ils créent souvent des logiciels malveillants spéciaux que votre antivirus ne peut pas détecter. Ils contournent vos filtres de messagerie avec une attaque de phishing personnalisée ou vous appellent au téléphone pour vous piéger ou vous arnaquer à partir de votre carte de crédit, de votre argent ou de votre mot de passe. La technologie joue un rôle important dans votre protection, mais vous êtes en définitive la meilleure défense.

Heureusement, être en sécurité n'est pas si difficile; au final, le bon sens et certains comportements de base constituent votre meilleure défense. Si vous recevez un courrier électronique, un message ou un appel extrêmement pressant, étrange ou suspect, il peut s'agir d'une attaque. Pour vous assurer que vos ordinateurs et vos périphériques sont sécurisés, maintenez-les à jour et activez la mise à jour automatique. Enfin, utilisez une phrase de passe puissante et unique pour chacun de vos comptes. Rester cyber-conscient est finalement votre meilleure défense. Vous ne savez pas par quoi commencer? Pensez à vous abonner à la newsletter mensuelle OUCH! sur sans.org/ouch.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Matt Bromiley *(@mbromileyDFIR) est responsable en gestion des incidents et expert en recherche de preuves numériques avec plus de 8 ans d'expérience. Il a travaillé avec des organisations sur des incidents à travers le monde. Matt est également un instructeur en criminalistique numérique et intervenant en cas d'incident, enseignant à la fois les cours SANS FOR508 et FOR572.*

SANS SECURITY AWARENESS

Sources

Arrêtez les logiciels malveillants :	https://www.sans.org/u/L1J
Ingénierie sociale :	https://www.sans.org/u/L1O
Attaques téléphoniques & escroqueries :	https://www.sans.org/u/L1T
Phrases de passe :	https://www.sans.org/u/L1Y
Poster – Vous êtes une cible :	https://www.sans.org/u/L23

Comité de rédaction : Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Traduit par : Marilyn Combet