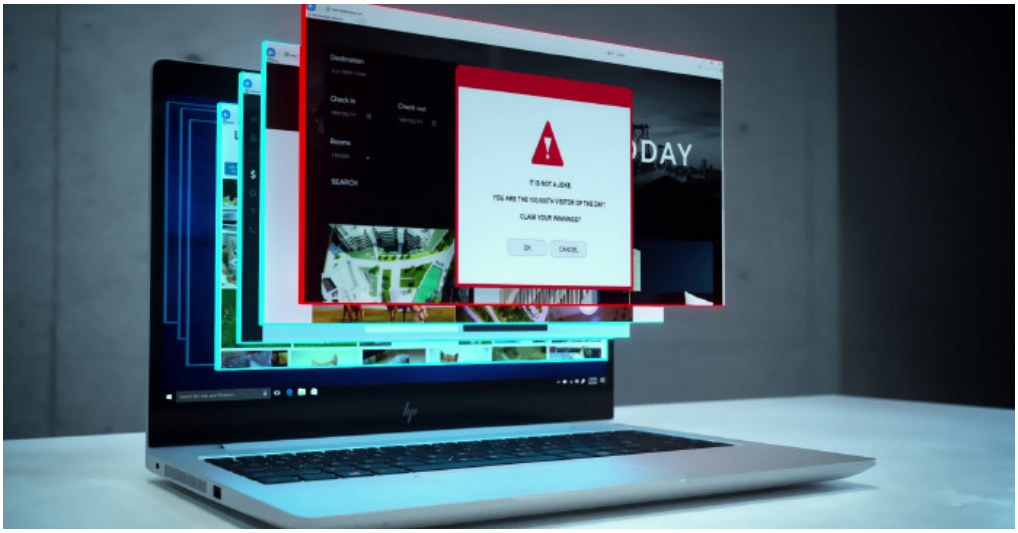
La suplantación de identidad ya no solo ocurre en los correos electrónicos

Más información



Los navegadores web son un portal a un mundo de información... y de amenazas. ¿Qué puede hacer al respecto para proteger su negocio?

Los navegadores web tienen mucho ante lo que responder. En una encuesta reciente a 400 CIO, el 68 % afirmó que ahora los piratas son tan sofisticados que su personal tiene problemas para diferenciar entre los sitios web seguros y los que no lo son[1]. Teniendo en cuenta esto, no nos sorprende que el 70 % de los profesionales de TI sufran ataques de suplantación de identidad cada semana, y no solo por correo electrónico[2]. Los sofisticados hackers ahora emplean las redes sociales, anuncios y sitios web con errores ortográficos comunes para engañar a los empleados y hacer que revelen información personal sensible. A medida que los fraudes de suplantación de identidad se vuelven cada vez más difíciles de reconocer, los negocios se ven en aprietos a la hora de proteger a su plantilla frente a estos ataques.

A pesar de una mayor concienciación e inversión en software de seguridad y formación para empleados, ha habido un aumento del 232 % en ciberataques en portátiles y ordenadores de sobremesa en los últimos seis años[3]. Los piratas siguen colándose porque los números están de su parte. Proteger sus datos conlleva un esfuerzo enorme, pero basta que un solo empleado haga clic en un enlace malicioso para que su negocio se vaya al garete.

Los ciberataques en las redes sociales son gran parte del problema. Las plataformas como Facebook y Twitter son un próspero coto de caza para los piratas. No solo están diseñadas para fomentar la participación y la comunicación, sino que también son fáciles de usar y manejar. Es increíblemente sencillo crear cuentas fraudulentas y publicar contenido malicioso, desde enlaces y recopilación de datos hasta páginas de inicio con ventanas emergentes poco fiables.

La mayoría de estas actividades en línea se basan en técnicas de suplantación de identidad, que solían limitarse a los correos electrónicos. Las redes sociales facilitan la conexión entre personas, y no supone mucho esfuerzo crear un personaje creíble con el que contactar con usuarios auténticos de las plataformas.

Vevo, el servicio de retransmisión, es una víctima reciente de una filtración de datos masiva. Uno de sus empleados se convirtió en objetivo de un fraude de suplantación de identidad en LinkedIn, el cual derivó en una filtración en línea de 3,12 TB de archivos internos. Estos incluían vídeos, documentos de oficina, material promocional, contenido de redes sociales aún sin publicar e información sobre artistas de las compañías discográficas participantes[4].

El grupo pirata OurMine reivindicó el ataque tras una trifulca por correo electrónico con un miembro del personal de Vevo. Esto demuestra el peligro del **phishing dirigido**, un ataque específico que trata de robar datos de un objetivo concreto. Los hackers suelen adoptar la forma de un amigo o una fuente fiable (como su banco) para engañar a la víctima y hacer que comparta información, lo cual se produce en el 91 % de los ataques.

La suplantación de identidad ya no solo ocurre en los correos electrónicos

Para la mayoría de los negocios víctima de un ataque de suplantación de identidad, como Vevo, las consecuencias son tanto perjudiciales como duraderas. No solo pueden suponer la pérdida de la productividad de los empleados y de los datos de los clientes, sino también la pérdida de los clientes en sí. La confianza que sus clientes tienen en su negocio podría desmoronarse a causa de un fallo de seguridad, pues consideran que su información ya no está segura con usted. Y, aunque es posible evitarlo, en gran parte de los casos las implicaciones son permanentes.

En el cuarto trimestre de 2017, los ataques de suplantación de identidad en las redes sociales aumentaron en un 500 %, con una tendencia de cuentas falsas que fingían ser un servicio de atención al cliente de grandes marcas[5]. Este acontecimiento se denominó **suplantación de identidad del pescador**, ya que los hackers lanzaban un anzuelo y esperaban a que los usuarios de redes sociales se les acercaran. Al usar la misma imagen de marca y un nombre de cuenta de aspecto auténtico, millones de personas que confían en las redes sociales se ven engañadas ante un ataque convincente. Es entonces, tan pronto como el usuario establece un contacto, cuando la cuenta falsa le envía un enlace a un sitio web de suplantación de identidad y le pide que inicie sesión, lo cual permite que el hacker alcance su objetivo final: obtener información privada.

Una de las maneras más sencillas de evitar que sus empleados caigan en la suplantación de identidad a través de las redes sociales es promoviendo un cambio de comportamiento en el trabajo. Esto debería evitar que su personal cometa errores simples que deriven en consecuencias devastadoras para su negocio:

1. Limite las interacciones a usuarios en los que confía
2. No haga clic en enlaces de fuentes sin confirmar
3. Nunca descargue archivos adjuntos de las redes sociales
4. Habilite la autenticación de doble factor en todas las cuentas de redes sociales y dispositivos, pues dificultará que sean hackeadas
5. Ofrezca formación adicional a los empleados con acceso privilegiado a perfiles en las redes sociales

Otro aspecto esencial de su plan de seguridad consiste en analizar la tecnología que emplea para aumentar la resistencia cibernética de su empresa. La familia HP Elite, por ejemplo, se compone de portátiles y ordenadores de mesa diseñados desde cero pensando en la seguridad.

Una de sus características es HP Sure Click, disponible en plataformas HP Elite seleccionadas, que trata la navegación segura desde otra perspectiva. En lugar de simplemente alertar sobre sitios web peligrosos que los usuarios deberían eludir, también evita que el malware, el ransomware y los virus infecten otras pestañas del navegador y más partes del sistema. Cuando un usuario inicia una sesión en su navegador, cada sitio web visitado activa HP Sure Click. Por ejemplo, cada vez que se visita un sitio web, HP Sure Click crea una sesión de navegación aislada basada en hardware, que elimina la capacidad de un sitio web de infectar otras pestañas o el mismo sistema.

Cuando se trata de que un negocio cambie su estrategia de seguridad y adquiera estos innovadores dispositivos, como la serie HP EliteBook 800, con procesadores opcionales Intel® Core™ de octava generación, suele ser más fácil decirlo que hacerlo. Ahí es donde entra en acción una solución como el Dispositivo como servicio (Device as a Service, DaaS) de HP. Es un modelo de consumo moderno para PC que simplifica la forma en que las organizaciones comerciales proporcionan a sus empleados hardware y accesorios adecuados, gestionan flotas de dispositivos con múltiples sistemas operativos, y obtienen servicios del ciclo de vida adicionales. HP DaaS ofrece planes sencillos a la vez que flexibles, a un precio por dispositivo para que todo funcione sin problemas y de manera eficiente.

En última instancia, un equipo bien formado y dispositivos con seguridad optimizada le ayudarán a enfrentarse al hackeo en las redes sociales, una de las mayores ciberamenazas en estos momentos. El futuro se presenta peor y más siniestro, por lo que ahora es el momento de mejorar sus defensas.

Para obtener más información sobre cómo proteger los dispositivos de su empresa, lea nuestro último descubra los beneficios para su negocio con las soluciones de seguridad de HP.

Fuentes:

1. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
2. https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/8355/HP-Nearly-70-of-IT-Professionals-Experience-Weekly-Phishing-Attacks.aspx
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. https://www.zerofox.com/blog/vevo-hacked-via-linkedin-phishing-campaign/
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

4AA7-3218ESE, Mayo de 2018