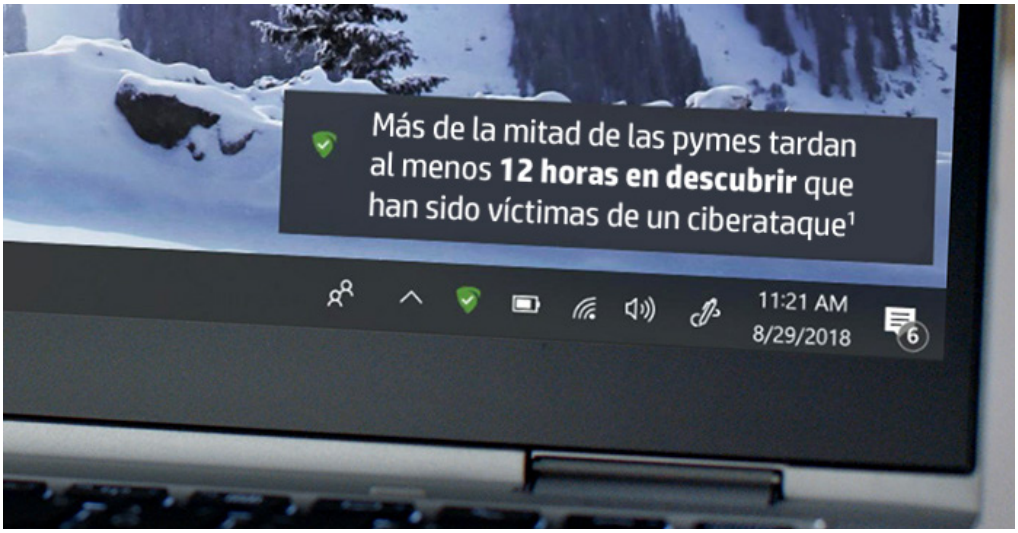
La suplantación de identidad ya no se limita a los correos electrónicos

Más información



Los navegadores web son un portal a un mundo de información... y de amenazas. ¿Qué puedes hacer para proteger tu 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[2]. Teniendo en cuenta esto, no nos sorprende que casi el 70 % de los profesionales de IT sufra ataques de suplantación de identidad cada semana, y no solo por correo electrónico[3]. 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 confidencial. 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 haber un mayor conocimiento e inversión en el software de seguridad y la formación de los empleados, el número de ciberataques en portátiles y ordenadores de sobremesa se ha incrementado en un 100 %[4]. Los piratas siguen colándose porque los números están de su parte. Proteger tus datos conlleva un esfuerzo enorme, pero basta que un solo empleado haga clic en un enlace malicioso para que tu negocio se vaya al garete.

Los ciberataques en las redes sociales son una parte importante 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.

Para la mayoría de los negocios que son víctimas de un ataque de suplantación de identidad, 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 tus clientes tienen en tu negocio podría desmoronarse a causa de un fallo de seguridad, pues consideran que su información ya no está segura contigo. Y, aunque es posible evitarlo, en gran parte de los casos las implicaciones son permanentes.

La suplantación de identidad ya no se limita a los correos electrónicos

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. Dado que se utiliza 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 confidencial.

Una de las maneras de evitar que tus 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 tu personal cometa errores simples que deriven en consecuencias devastadoras para tu negocio:

1. Limita las interacciones a usuarios en los que confías
2. No hagas clic en enlaces de fuentes sin confirmar
3. Nunca descargues archivos adjuntos de las redes sociales
4. Habilita la autenticación de doble factor en todas las cuentas de redes sociales y dispositivos, pues dificultará que sean hackeadas
5. Ofrece formación adicional a los empleados con acceso privilegiado a perfiles en las redes sociales

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

Una de sus características de seguridad es HP Sure Click[6], disponible en dispositivos portátiles y estaciones de trabajo HP Elite seleccionados, 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.

HP Sure Click incluso protege a los usuarios de malware infectado oculto en archivos PDF y de Office. Imaginemos que tus empleados han recibido un PDF infectado a través del correo electrónico. Podrían abrirlo de manera segura sabiendo que HP Sure Click lo aislará en un contenedor basado en hardware y evitará que se extienda la infección más allá del archivo. Con esta solución de seguridad incorporada a tu flota de ordenadores, las amenazas online dejarán de ser una preocupación.

Cuando se trata de que un negocio cambie tu estrategia de seguridad y adquiere estos innovadores dispositivos, como el HP EliteBook x360, con procesadores opcionales Intel® Core™ i7 de 8.ª generación, puede ser un poco complicado. Ahí es donde entra en acción una solución como el HP Device as a Service (HP DaaS)[7]. Se trata de un modelo de consumo moderno de ordenadores 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 te ayudarán a enfrentarte al hackeo en las redes sociales, una de las mayores ciberamenazas en estos momentos. Parece que la situación irá a peor, por lo que ahora es el momento de mejorar tus defensas.

Descubre las ventajas que ofrecen las soluciones de seguridad de HP a tu negocio.

Fuentes:

1. Informe Osterman, patrocinado por Malwarebytes “Second Annual State of Ransomware Report: US Survey Results”, julio de 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 está disponible en la mayoría de los ordenadores HP y es compatible con Microsoft® Internet Explorer, Google Chrome y Chromium™. Los adjuntos compatibles incluyen Microsoft Office (Word, Excel, PowerPoint) y archivos PDF solo en modo de lectura, cuando Microsoft Office o Adobe Acrobat están instalados.

7. Los planes y/o componentes de HP DaaS incluidos pueden variar según la región o el proveedor de servicios autorizado de HP DaaS. Contacta con tu representante local de HP o tu socio de DaaS autorizado para obtener información específica en tu ubicación. Los servicios HP se rigen por los términos y condiciones aplicables de HP que se proporcionan o indican al cliente en el momento de la compra. El cliente puede tener derechos legales adicionales según las leyes locales respectivas, los cuales no se ven afectados en modo alguno por los términos y condiciones de servicio de HP ni por la garantía limitada de tu producto HP.

© Copyright 2019 HP Development Company, L.P. La información aquí contenida está sujeta a cambios sin previo aviso.

4AA7-317ESES, abril de 2019