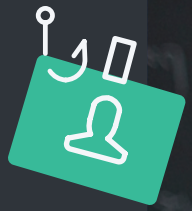
Phishing en K12

para principiantes



¡Saludos! Este es el segundo libro electrónico de nuestra serie sobre ciberseguridad en las escuelas K-12 (primaria y secundaria). En esta serie, vamos a hacer un recorrido por las amenazas más comunes para la ciberseguridad a las que se enfrentan las escuelas. **Nuestra primera parada fue el malware.**

Por mucho que nos gustaría prepararnos con nuestros carretes y cajas de aparejos, esta parada es un viaje de **pesca** de otro tipo. (N. de traducción: Es un juego de palabras en inglés, ya que "pesca" se dice "fishing" en inglés, y esta ciberamenaza se pronuncia de la misma forma.)

jamf

EN ESTE LIBRO ELECTRÓNICO HABLAREMOS DE:

¿Qué es el phishing?

"Phishing", o suplantación de identidad, es un término bastante antiguo, al menos durante la vida de Internet. Fue anterior a la invención del Wi-Fi y a la creación de sitios web como Google y Wikipedia. Al igual que la pesca fuera de línea a la antigua usanza, el phishing utiliza un cebo para atraer a los incautos hacia consecuencias desafortunadas.

El phishing se utiliza para recopilar datos como información bancaria, credenciales de inicio de sesión o información personal identificable (IPI), como la fecha de nacimiento o el número de la seguridad social. Es el método de ataque inicial más común, representando el 16% de las transgresiones de datos, según el **Informe IBM 2023: Cost of a Data Breach**. También es caro, ya que cuesta una media de $4.76 millones de dólares a la organización.

Por lo general, el phishing utiliza algunas tácticas comunes para que sea más probable que las víctimas muerdan el anzuelo:

Urgencia: Los atacantes suelen exigir atención inmediata, amenazando con la pérdida de una cuenta, sanciones por retraso en el pago, daños a un ser querido o algún tipo de consecuencia negativa. O pueden apelar a la amabilidad alegando que se encuentran en una situación vulnerable y que usted puede ayudarles.

Parecidos: Las URL de los sitios web pueden parecerse a las URL reales pero tener caracteres especiales. Los sitios web o correos electrónicos pueden estar cuidadosamente diseñados y que luzcan familiares, como un sitio web bancario o un correo electrónico de restablecimiento de contraseña.

Suplantación de identidad: Los hackers pueden hacerse pasar por personas conocidas utilizando su dirección de correo electrónico, su número de teléfono o incluso su voz, con lo que es más probable que usted responda a su intento de phishing.

Los atacantes utilizan estos métodos de ingeniería social por la sencilla razón de que no suelen requerir grandes conocimientos técnicos. Al fin y al cabo, es mucho más fácil engañar a alguien para que te dé los datos de acceso de su cuenta que probar todas las combinaciones de contraseñas hasta acertar.

Ingeniería social

La ingeniería social es una técnica de manipulación que utiliza el control psicológico y explota el error o la debilidad humana para obtener información privada, acceso u objetos de valor. A veces se denomina "piratería humana"

Tipos habituales de ataques de phishing

Los ataques de phishing adoptan varias formas comunes. Repasemos algunas de ellas.

PHISHING POR CORREO ELECTRÓNICO

Los atacantes envían un correo electrónico a un gran grupo de personas. Este correo electrónico puede contener un archivo adjunto que instale malware o un enlace que les lleve a un sitio web creado para robar sus datos de acceso.

SPEAR PHISHING

A menudo a través del correo electrónico, los atacantes se dirigen a ciertas personas o a pequeños grupos. Estos correos electrónicos tienen un contenido familiar para el destinatario. Por ejemplo, los estudiantes y profesores pueden recibir un correo electrónico que parece provenir de un software que utilizan para la escuela, pero que contiene enlaces a un sitio web malicioso.

CAZA DE BALLENAS

Estos ataques se centran en personas destacadas, como el director general de una empresa. Los atacantes podrían hacerse pasar por un socio comercial, solicitando dinero a través de una transferencia bancaria. O pueden hacerse pasar por un superintendente para obtener información de un director de escuela.

ABREVADERO

Un ataque de abrevadero (watering hole) es similar al spear phishing porque ambos desarrollan ataques para un objetivo específico. Sin embargo, un abrevadero no suele empezar por contactar con una persona. En su lugar, los atacantes piratean un sitio web donde se reúnen sus objetivos y lo modifican para que robe sus datos o ejecute malware.

SUPLANTACIÓN DE DNS

Cuando usted escribe la dirección de un sitio web en su navegador, el software del Sistema de Nombres de Dominio (DNS) traduce esa dirección en una serie de números exclusivos del sitio web. La suplantación de DNS engaña al software DNS cambiando los números. Esto significa que cuando usted teclea la dirección correcta en su navegador, el software DNS —ahora comprometido— le lleva al sitio de un atacante con la esperanza de que introduzca información.

SMISHING

El smishing combina "SMS" y "phishing", es decir, es un phishing que se lleva a cabo mediante mensajes de texto. Esto puede ser difícil de detectar, ya que los enlaces en los textos a menudo se acortan o son difíciles de previsualizar.

Las personas también utilizan sus dispositivos móviles cuando tienen prisa o están en movimiento, por lo que es menos probable que se tomen el tiempo necesario para verificar el enlace.

VISHING

Vishing es una combinación de "voice" (voz) y "phishing" (suplantación de identidad), es decir, suplantación de identidad que utiliza la voz de alguien. Puede ser la voz de un desconocido por teléfono, que puede apelar a la amabilidad de la gente. O, con los avances en inteligencia artificial (IA), puede ser incluso la voz de un ser querido, pidiéndole urgentemente que le envíe dinero.

Cómo afecta el phishing a los centros de enseñanza primaria y secundaria

El K12 Security Information eXchange (K12 SIX) ofrece orientación sobre ciberseguridad a los centros escolares. En su mapa de incidentes, K12 SIX enumera los incidentes de ciberseguridad que sufrieron las escuelas K-12 de Estados Unidos entre 2016-2022. He aquí algunos ejemplos de cómo el phishing ha afectado a los centros escolares:

Se enviaron a los profesores correos electrónicos con un enlace de phishing, lo que permitió a los delincuentes **desviar los depósitos directos de los profesores** y dar lugar a un robo de nóminas por valor de más de $50,000 dólares.

Un atacante que se hizo pasar por contratista del distrito engañó a empleados del distrito para que **transfirieran $2.9 millones de dólares a su cuenta.** Afortunadamente, esto se ha recuperado.

Un profesor accede a un correo electrónico de un **atacante que se hace pasar por su compañero de trabajo** y le pide $500 dólares en tarjetas de regalo.

Haciéndose pasar por administradores escolares, los atacantes enviaron correos electrónicos al personal de nóminas y/o recursos humanos **solicitando información sobre el formulario W-2 de los** empleados, y un gran número de escuelas fue víctima de esta solicitud.

Un alumno utiliza el spear phishing creando una cuenta de correo electrónico en la que se hace pasar por un alto cargo de la administración y solicita información de acceso a varios profesores. A continuación, el alumno utiliza esta información para mejorar sus calificaciones y reducir las de los demás estudiantes.

Un tema común en estos ataques está relacionado con los correos electrónicos que parecen proceder de una fuente de confianza. Puede tratarse de correos electrónicos creados por atacantes con diferencias ortográficas apenas perceptibles o de correos electrónicos comerciales comprometidos, en los que los atacantes acceden a la cuenta de correo electrónico real.

Aunque estos ataques se centran principalmente en el profesorado y el personal, los datos de los estudiantes también se ven afectados. El phishing es una forma habitual en que los atacantes inician los ataques de ransomware, que ocasionan filtraciones de datos que pueden perseguir a los estudiantes años después de que se produzca el ataque. Los atacantes pueden utilizar la información de un estudiante para pedir préstamos o abrir tarjetas de crédito, por poner solo dos ejemplos. Estos estudiantes, muchos de ellos jóvenes, no pueden o no sabrán comprobar sus informes crediticios hasta muchos años después de que se haya producido el ataque.

PREVENCIÓN DEL PHISHING

El phishing puede ser difícil de prevenir. Las escuelas pueden poner todo tipo de defensas, solo para que alguien dé a un atacante su información de acceso.

¡Pero no toda la esperanza está perdida!

Veamos algunas formas en que los centros escolares pueden luchar contra la amenaza siempre presente del phishing.

Educación de los usuarios

Dado que el phishing suele basarse en la ingeniería social, los usuarios capaces de identificar y detener los ataques de phishing constituyen la primera línea de defensa. Al fin y al cabo, si los usuarios nunca hacen clic en enlaces de phishing, no descargan archivos adjuntos maliciosos ni obedecen las peticiones de un atacante, ¡muchos ataques de phishing no tendrán éxito!

Consejo:

Lleve la educación sobre phishing a las aulas

He aquí algunos temas a tratar:

Qué es el phishing

El phishing es un tipo de estafa en la que los atacantes se hacen pasar por alguien o algo que no son, con el fin de recabar información privada. Los agresores pueden hacerse pasar por un amigo, un familiar, un compañero de trabajo o una persona con autoridad. O pueden hacerse pasar por su banco, una empresa en la que tenga una cuenta como Google, Apple o Microsoft, u otra institución que pueda tener su información. La suplantación de identidad se realiza habitualmente por correo electrónico, pero puede producirse a través de mensajes de texto, redes sociales, llamadas telefónicas o en persona. Puede que los atacantes ni siquiera se pongan en contacto con usted directamente, sino **pueden publicar algo en las redes**sociales a través de la cuenta de uno de tus amigos.

Qué hacer si sospecha de un intento de phishing

Si recibe un correo electrónico sospechoso, lo primero que debe hacer es **no hacer clic en nada**, es decir, ni en enlaces ni en archivos adjuntos. Si se trata de un correo electrónico de la escuela, debe informar del correo electrónico a su departamento de IT. Algunas escuelas tienen un botón que lo permite hacerlo fácilmente.

Cómo es el phishing

Un ataque de phishing puede intentarse por correo electrónico, mensaje directo, texto, llamada, en un sitio web o en persona. Aunque no hay dos ataques exactamente idénticos, hay algunas señales a las que hay que prestar atención:

- Un mensaje o una llamada de alguien conocido a una hora extraña del día o de la noche.
- Una sensación de urgencia, como una exigencia de pago o que se está produciendo una emergencia.
- Direcciones de correo electrónico o de sitios web que se parecen **mucho** a las conocidas, pero son ligeramente diferentes. Pueden tener caracteres especiales o sustituir a otros caracteres: por ejemplo, puede utilizar "0" en lugar de "O". Tenga en cuenta que los correos electrónicos también pueden ser totalmente legítimos pero seguir siendo phishing si la cuenta del remitente ha sido tomada por atacantes.
- Si algo es demasiado bueno para ser verdad, por ejemplo, todo lo que tienes que hacer es darles algunos datos y ¡obtendrás una tarjeta regalo de $100!
- Peticiones inesperadas, como si un correo electrónico que parece de un amigo quiere saber tu dirección, fecha de nacimiento u otra información personal.

Filtrado de contenidos

Desgraciadamente, la educación de los usuarios tiene un límite. Las personas no son infalibles, y basta un intento para que los atacantes consigan acceder. Ahí es donde el filtrado de contenidos puede ayudar.

El filtrado de contenidos bloquea esencialmente el acceso a sitios web maliciosos. Por ejemplo, si un usuario se equivoca y hace clic en un enlace de phishing en un correo electrónico, un filtro de contenidos lo reconocerá e impedirá el acceso al enlace.

Un filtro de contenidos puede funcionar de varias maneras. Una forma es tener una lista de sitios permitidos/bloqueados, en la que los administradores de IT permiten o bloquean explícitamente los sitios web de una lista. Esto funciona, pero la implementación más segura implica tener una lista corta de sitios permitidos, que bloquea una enorme porción de Internet. Este método impide que los alumnos exploren libremente; al fin y al cabo, cuando salgan de la escuela, esta será la versión de Internet a la que tendrán acceso.

Un método mejor es el filtrado de contenidos que utiliza inteligencia artificial (IA) y aprendizaje automático (ML). En lugar de reducir Internet a un puñado de sitios web, la IA y el ML pueden determinar de forma inteligente si es seguro acceder a un sitio sin que un administrador de IT tenga que permitirlo o bloquearlo explícitamente. Esto no solo permite acceder a una mayor parte de la web, sino que también bloquea los sitios web amenazadores que aún no se han descubierto. Este método da a los alumnos libertad para explorar, pero con límites. **Esto ayuda a enseñar a los alumnos a ser ciudadanos digitales seguros incluso una vez que dejan la escuela.**

Inicio de sesión único

El inicio de sesión único (SSO) permite a los usuarios conectarse sin tener que recordar una contraseña para todas sus cuentas de Internet. Incluso puede configurarse para que los usuarios puedan iniciar sesión utilizando su huella dactilar. En otras palabras, solo tiene que recordar su contraseña de SSO, y su proveedor de SSO iniciará sesión en el resto de sus cuentas por usted.

Esto ayuda a prevenir el phishing de dos maneras. SSO solo funciona para los sitios web y las cuentas que ha guardado. Si hace clic en un enlace de phishing, su proveedor de SSO no reconocerá el sitio web y no transferirá ninguna información suya a los atacantes. Dado que el SSO puede requerir el uso de una huella digital para iniciar sesión, esto actúa como un factor adicional de autenticación. Esto hace que sea más difícil para los atacantes acceder con éxito a su cuenta.

Administración de dispositivos

La administración de dispositivos es una parte necesaria de la seguridad de los dispositivos de un centro escolar. Al inscribir todos los dispositivos que acceden a los recursos de la escuela en una solución de administración de dispositivos móviles (MDM), los administradores de IT obtienen mucha visibilidad de la situación de seguridad de un dispositivo.

Para tener algo como el filtrado de contenidos en un dispositivo, es necesario empezar por inscribirse en una solución MDM. El software de la MDM ofrece a los administradores la posibilidad de configurar los dispositivos, incluso restringiendo determinados ajustes o añadiendo software de filtrado de contenidos.

Autenticación multifactor

La autenticación multifactor (MFA) es una excelente forma de reducir las posibilidades de que tenga éxito un intento de phishing. La MFA requiere dos métodos de autenticación de estos:

- **Algo que conozca,** como una contraseña, un PIN o una pregunta de seguridad
- **Algo que sea parte de usted,** como su huella digital o su rostro
- **Algo que tenga,** como otro dispositivo o clave de seguridad

Un ejemplo común es cuando teclee su contraseña (algo que sabe) y recibe un texto con un código de seis dígitos en un dispositivo de confianza (algo que tiene).

He aquí un escenario en el que la MFA sería de ayuda:

1. Recibió un correo electrónico invitándole a un documento de Google compartido. (¡No se da cuenta de que es un correo de phishing!)

2. Hace clic en el enlace, que le lleva a un sitio parecido a la página de inicio de sesión de Google.

3. Introduce sus datos, pero nunca accede a dicho documento.

4. ¡Los atacantes ya tienen su información! Más tarde, intentan acceder a su cuenta.

5. Aparecerá un mensaje MFA que le pedirá que apruebe la solicitud de inicio de sesión.

6. Dado que la solicitud procede de un lugar extraño o en un momento en el que no está intentando iniciar sesión, usted rechaza la solicitud.

Los atacantes no pueden acceder a su cuenta.

No se trata de un **tipo hipotético de estafa de phishing**, sino que es una que se ha utilizado una y otra vez. En un entorno educativo colaborativo, la gente puede caer especialmente en este ataque, ya que este tipo de correo electrónico puede ser común o esperado.

IMPLEMENTACIÓN: JAMF SCHOOL Y JAMF SAFE INTERNET

Ya hemos hablado de varias formas de prevenir el phishing. Hablemos ahora de su implementación.

Jamf School

Hablando de administración de dispositivos, **Jamf School** ofrece una versión de MDM creada especialmente para escuelas. Ofrece:

- Inventario de dispositivos para que los administradores sepan qué dispositivos están conectados a los recursos de la escuela
- Transparencia sobre el estado de los dispositivos para poder resolver rápidamente cualquier problema
- La posibilidad de establecer restricciones y ajustes en un dispositivo, incluido un código de acceso obligatorio
- Compatibilidad con un SSO (con un proveedor de identidad adicional)
- Una forma sencilla de que los profesores soliciten la aprobación de IT para las aplicaciones
- ¡Y mucho más!

Las capacidades de administración de Jamf School crean una base sólida para dispositivos seguros, con funciones como SSO y configuración de dispositivos que reducen el impacto que podría tener un intento de phising.

Jamf Safe Internet

Jamf Safe Internet lleva la seguridad un paso más allá y es compatible con dispositivos Apple, Chromebook y Windows. Jamf Safe Internet es totalmente personalizable, lo que facilita el establecimiento o cambio de políticas para diferentes grupos de dispositivos en función de su geografía, tipo u otros atributos. Funciona con dispositivos tanto si viven en un carrito, son asignados 1:1 por la escuela o si son dispositivos propios del alumno.

Para defenderse de amenazas como el phishing, Jamf Safe Internet ofrece:

- **Potente filtrado de contenidos** respaldado por IA y ML: bloquea el acceso a sitios web de phishing incluso antes de que se descubran como maliciosos
- **DNS y bloqueo de nombres de dominio** para defenderse de la suplantación de DNS
- **Filtrado de contenidos para dispositivos** como el iPad, para filtrarlos en cualquier lugar
- **Protección en red** contra sitios web maliciosos antes de que puedan afectar a los dispositivos
- **Google SafeSearch y Google Safe Browsing obligatorios** para evitar que aparezcan sitios maliciosos o inapropiados en las búsquedas

Toda esta **seguridad sin vigilancia:** los alumnos son libres de navegar por Internet y desarrollar sus competencias de ciudadanía digital sin violar su intimidad.