Phishing

Phishing

EnorChile

¿Qué es y en qué consiste el phishing?

EnorChile

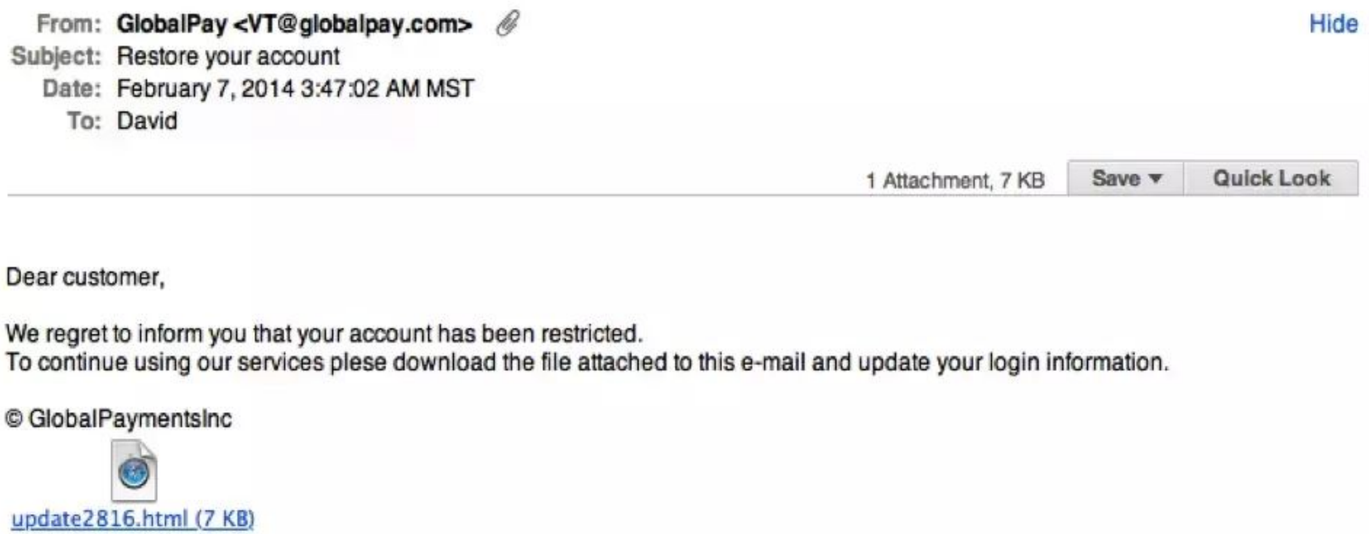
El phishing es un tipo de fraude, que consiste en el envío de un correo electrónico por parte de un ciberdelincuente simulando ser una entidad o persona de confianza para la persona que lo recibe.

El 95% de todos los ataques a redes empresariales son el resultado de un phishing dirigido con éxito. - Instituto SANS

¿Cómo reconocer el phishing?

EnorChile

Algunos indicadores comunes de phishing incluyen comunicaciones inesperadas solicitando información personal o financiera, direcciones de correo electrónico del remitente desconocidas, saludos genéricos, errores de ortografía y gramática, y URLs engañosas. Siendo cautelosos y verificando cualquier comunicación sospechosa directamente con las instituciones involucradas antes de responder, los individuos pueden protegerse mejor contra los intentos de phishing. Ahora queremos profundizar más en las señales de phishing y ayudarte a identificarlas.



Señales de phishing

EnorChile

Señal 1: El correo electrónico presenta una oferta que parece demasiado buena para ser verdad.

Podría afirmar que te has sacado el premio gordo, ganado un premio extravagante u otras recompensas improbables.

Señal 2: El remitente es reconocible, pero no alguien con quien normalmente interactúas.

Incluso si reconoces el nombre del remitente, ten precaución si no es alguien con quien normalmente te comunicas, particularmente si el contenido del correo electrónico no está relacionado con tus tareas habituales. Del mismo modo, ten cuidado si estás en copia en un correo electrónico junto a individuos desconocidos o colegas de departamentos no relacionados.

Señal 3: El mensaje induce miedo.

Ten cuidado si el correo electrónico utiliza un lenguaje cargado o alarmante para infundir una sensación de urgencia, instándote a hacer clic y "actuar de inmediato" para evitar la cancelación de la cuenta. Recuerda, las organizaciones legítimas no solicitarán información personal por correo electrónico.

Señal 4: El mensaje incluye archivos adjuntos inesperados o extraños.

Estos archivos adjuntos pueden contener malware, ransomware u otras amenazas en línea.

Señal 5: El mensaje incorpora enlaces que parecen dudosos.

Incluso si los indicadores anteriores no suscitan sospechas, nunca confíes ciegamente en los hipervínculos incrustados. Pasa el cursor sobre el enlace para revelar la URL real. Presta especial atención a los sutiles errores tipográficos en una URL de un sitio web aparentemente familiar, ya que es una señal de engaño. Siempre es más seguro ingresar manualmente la URL en tu navegador en lugar de hacer clic en el enlace incrustado.

¿Cómo protegerte contra los ataques de phishing?

EnorChile

No abras correos electrónicos de remitentes que no conoces.

Nunca hagas clic en un enlace dentro de un correo electrónico a menos que sepas exactamente a dónde te lleva.

Si se te pide que proporciones información confidencial, verifica que la URL de la página comience con "HTTPS" en lugar de solo "HTTP". La "S" significa "seguro". No es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos usan HTTPS porque es más seguro. Los sitios HTTP, incluso los legítimos, son vulnerables a los hackers.

Habilita la Autenticación Multifactor (MFA): Utiliza MFA siempre que sea posible para añadir una capa adicional de seguridad. Incluso si los phishers obtienen tu contraseña, necesitarán eludir pasos de verificación adicionales para acceder a tu cuenta.

Observa el certificado digital de un sitio web.

Para añadir esa protección, si recibes un correo electrónico de una fuente de la que no estás seguro, navega al enlace proporcionado manualmente ingresando la dirección web legítima en tu navegador.

Pasa el ratón sobre el enlace para ver si es un enlace legítimo.

Si sospechas que un correo electrónico no es legítimo, toma un nombre o parte del texto del mensaje e introdúcelo en un motor de búsqueda para ver si existen ataques de phishing conocidos que utilizan los mismos métodos.

Ransomware

Qué es Ransomware

EnorChile

El ransomware es una clase de malware que representa un riesgo para ti y para tu dispositivo. ¿Sabes qué lo hace tan especial? Su nombre no es casualidad: el término con el que comienza, “ransom”, es una palabra inglesa que significa “rescate”. El ransomware es un software extorsivo: su finalidad es impedirte usar tu dispositivo hasta que hayas pagado un rescate.

Cómo detectar el ransomware y qué hacer para protegerse

EnorChile

En lo que respecta al ransomware, es mejor prevenir que curar. Ello significa tener siempre un ojo atento y usar el software de seguridad adecuado. Los análisis de vulnerabilidades pueden ayudar a revelar si hay un intruso en el sistema. Es importante que el equipo no sea un blanco ideal para el ransomware. Las aplicaciones instaladas deben tener siempre las últimas actualizaciones y parches de seguridad. También es fundamental proceder con cautela, en especial al abrir archivos adjuntos o visitar sitios extraños. Pero como a veces la prevención no basta, contar con un plan de contingencia es fundamental. En el caso del ransomware, el plan consiste en tener copias de seguridad de los datos almacenados en el equipo.

¿Cuántas clases diferentes de ransomware existen? ¿Importa la diferencia?

EnorChile

Como dijimos, el riesgo del ransomware depende del tipo de virus. Existen, básicamente, dos clases de ransomware: el ransomware de bloqueo, por un lado, y el ransomware de cifrado, por el otro. Se diferencian de este modo:

- el ransomware de bloqueo afecta las funciones básicas del equipo,
- el ransomware de cifrado cifra archivos individuales.

El tipo de malware importa no solo por lo que hace, sino también porque afecta el modo de identificarlo y de contrarrestar sus efectos. Las dos clases generales se dividen, a su vez, en distintos tipos de ransomware. Algunos ejemplos de ransomware son **Locky**, **WannaCry** y **Bad Rabbit.**

Ejemplo

EnorChile

Phishing y Ransomware