Preview: The Bridge: March 9 Phishing Takeover

duphish@du.edu <duphish@du.edu>
Thu 3/9/2023 3:34 PM
To: Kelsey Bingham <Kelsey.Bingham@du.edu>

Phishing Takeover

UNIVERSITY OF DENVER • The Bridge

In this edition:

Campaña de ciberseguridad "Catch-a-Phish" del Departamento de IT de DU

En caso de que usted se lo haya perdido en las últimas semanas, aquí está un resumen de nuestra campaña de ciberseguridad llamada "Catch-a-Phish".

Es un nuevo año y con él llegan nuevas sorpresas. Es posible que en las últimas semanas usted haya visto unos perritos disfrazados de pescados rondando por el campus de DU.

Estos perritos fueron usados para promover la campaña con la colaboración de Colorado Saint Bernard Rescue. Los perritos nos ayudaron a atraer a la comunidad de DU para que participaran en los concursos de educación sobre el phishing para ganar premios y aprender a no caer en estafas de correo electrónico.

Es posible que usted esté familiarizado con el termino phishing, la práctica fraudulenta de enviar mensajes de correo electrónico simulando proceder de fuentes de confianza y a menudo engañando a las personas para que revelen información personal, como contraseñas o números de tarjetas de crédito. Por desgracia, una vez que los estafadores tienen sus contraseñas u otra información personal, estas violaciones de seguridad pueden causar importantes costos financieros para usted y toda la institución.

Empezamos nuestra campaña de ciberseguridad con un cuestionario inicial sobre phishing para poner a prueba los conocimientos básicos de ciberseguridad y phishing de nuestra comunidad de DU, y cada semana introducimos nuevos cuestionarios en

forma de concursos.

¿Todavía no ha tenido la oportunidad de participar en los cuestionarios o simplemente quiere un resumen? Todos los cuestionarios anteriores se pueden encontrar en nuestra página principal de Catch the Phish aquí.
¡Disfrute de estas fotos de nuestro campus participando en esta campaña!

Gracias al Colorado Saint Bernard Rescue

Las divisiones MarComm e IT de DU están muy agradecidas a la organización Colorado Saint Bernard Rescue por asociarse con nosotros y ayudarnos con esta campaña de phishing.

Colorado Saint Bernard Rescue es una organización de rescate basada en la categoría 501c3, formada exclusivamente por voluntarios y dedicada a la rehabilitación y búsqueda de hogares permanentes para perros de raza San Bernardo y mezcla de San Bernardo en Colorado. Desde 1997, se han dedicado a ayudar a la raza San Bernardos que son

abandonados, descuidados y maltratados, atendiendo todas sus necesidades (tanto médicas como de entrenamiento) con el fin de encontrarles el hogar perfecto.

Y ahora, ¡a conocer a nuestros amiguitos!

Consejo sobre phishing #1

Una de las formas más fáciles de reconocer un correo electrónico fraudulento es la mala gramática y la mala ortografía. Un correo electrónico de una organización legítima debería (casi siempre) estar escrito de forma profesional. De hecho, algunas empresas llegan incluso a enviar otro correo electrónico para corregir un error si creen que afectará su decisión de compra.

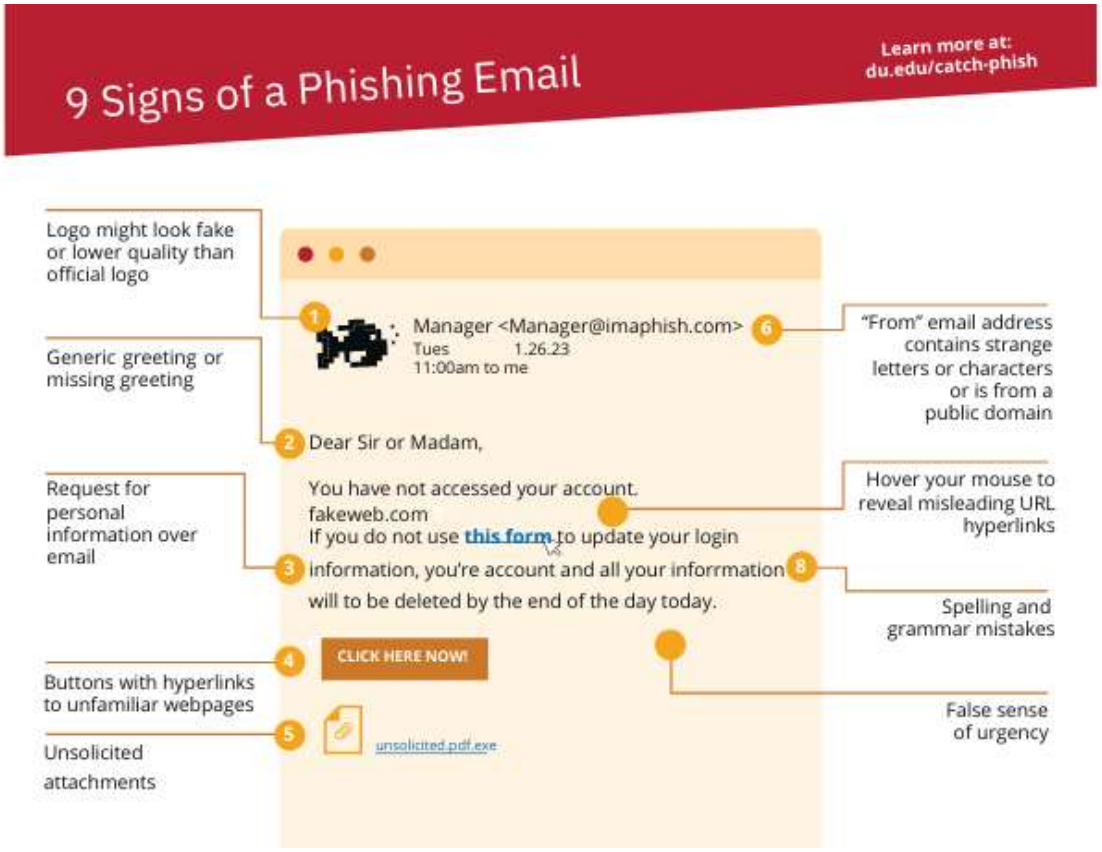
Es importante recordar que nunca hay que actuar sobre la base del propio correo electrónico: espere a ver si la "compañía de la tarjeta de crédito" o el "pariente lejano" le llama por teléfono o se pone en contacto con usted de alguna otra forma.

O mejor aún: llame al número que aparece en el reverso de su tarjeta de crédito, al número publicado en el sitio web oficial de la empresa, o a su pariente que conoce todo su árbol genealógico, para ver si el correo electrónico puede ser legítimo.

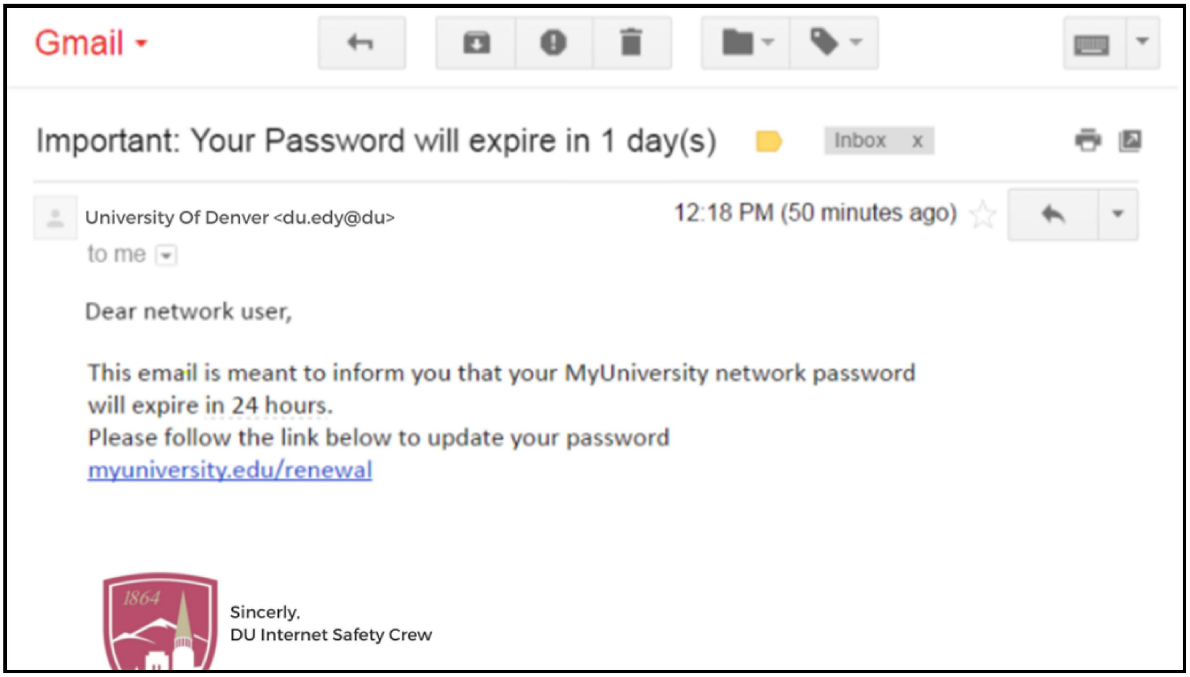
8 formas de detectar un intento de phishing

Los datos publicados por Proofpoint en el 2022 revelaron que el 80% de los participantes experimentaron un ataque de phishing por correo electrónico en el 2021, un aumento del 46% desde el 2020.

Para asegurarse de que está a salvo de estos estafadores, hemos creado este gráfico con las ocho formas más comunes de detectar un intento de phishing. Consulte este gráfico atentamente para asegurarse de que está preparado en caso de que un intento de phishing se cruce en su camino.



¿Cuál de las siguientes podría ser una estafa empleada por un estafador?



- Su cuenta bancaria ha sido comprometida y debe acceder al enlace indicado para restablecerla.
- Su paquete no puede ser entregado y debe acceder al enlace indicado con su dirección correcta.
- Su cuenta de redes sociales no ha tenido actividad reciente, y debe iniciar sesión en el enlace suministrado para reactivarla.
- Su devolución de impuestos está lista y debe conectarse al enlace indicado para recibirla.
- Usted pagó por una suscripción que no recuerda haber pedido, y debe llamar a un número indicado para cancelarla.
- Un viejo amigo le envía un correo electrónico con un enlace que afirma que usted le pidió.
- Su tarjeta de crédito ha sido rechazada y debe actualizar sus datos de facturación en el enlace indicado.
- Su información de iCloud falta o está incompleta, y debe iniciar sesión en el enlace indicado para proporcionarla.
- Se le ha pedido que complete una encuesta y debe hacer clic en el enlace indicado.
- Se le ha enviado una solicitud de Google Docs y debe hacer clic en el enlace para acceder a sus documentos de Google Docs.
- Usted recibe un mensaje de voz en forma de archivo .wav dentro de su correo electrónico, pero no contiene ninguna otra información y debe descargar el mensaje de voz para abrirlo.
- Usted recibió una factura, y debe hacer clic en el enlace incluido para pagarla.
- Recibe un correo electrónico en el que se le pide que actualice su cuenta de correo electrónico iniciando sesión en el enlace indicado.
- Recibe un archivo de Dropbox para revisar, y debe hacer clic en el enlace para revisar el archivo.
- Recibe un correo electrónico que parece ser del rector pidiéndole que complete una tarea, normalmente para comprar algo o descargar un archivo adjunto.
- Recibe un correo electrónico de una conocida empresa de venta al por menor en el que se le informa de que ha dejado artículos en su carro de la compra en línea y que debe hacer clic en el enlace suministrado para comprarlos.

Si usted ha adivinado todo esto, ¡está en lo cierto! Todos estos son ejemplos de intentos de phishing que hemos visto, y el cielo es el límite en lo que estos estafadores pensarán en el futuro.

Recuerde buscar estos ocho signos reveladores de un intento de robo de identidad cada vez que reciba un correo electrónico en el que se le solicite información personal. Los delincuentes no dejan de idear nuevas formas de engañarle, así que no caiga en su trampa.

¿Accidentalmente ha abierto un correo electrónico estafador?

Así que usted ha abierto accidentalmente un correo electrónico de estafa, y probablemente se está preguntando: ¿es malo? Y si es así, ¿qué tan malo es?

La buena noticia es que abrir un correo sospechoso, aunque no es lo ideal, es relativamente inofensivo. Los correos electrónicos de spam sólo se convierten en una ciberamenaza grave si ha cometido alguna de las siguientes acciones:

- Descargar archivos maliciosos o adjuntos al correo electrónico.
- Ha respondido con información confidencial (como los números de su tarjeta de crédito o de su cuenta bancaria).
- Ha hecho clic en enlaces adjuntos al mensaje.

¿Qué debo hacer después de abrir un correo electrónico de phishing?

Si ha abierto un correo electrónico de phishing pero no ha hecho clic ni descargado nada, asegúrese de hacer lo siguiente:

No se limite a cancelar la suscripción. Márquelo como correo no deseado para que su cliente de correo electrónico pueda hacer un mejor trabajo enviando los correos maliciosos directamente a su carpeta de spam.

Escanee su computadora en busca de ransomware, virus troyanos y otros programas maliciosos por si acaso. Los estafadores pueden utilizarlos para piratear su cuenta de correo electrónico.

Denuncie el mensaje al departamento de informática y cuéntele a sus amigos y familiares sobre la estafa para que sepan que también deben evitarla.

No entre en contacto con ningún correo de aspecto sospechoso y nunca respondas directamente.

Datos que hay que saber sobre el malware

El phishing no siempre es un enlace que le lleva a un sitio para robar su información personal. A veces, los propios correos electrónicos pueden contener lo que se llama malware. El malware es un programa diseñado para dañar su computadora y/o robar sus datos personales. Puede descargarse en su computadora disfrazado como un archivo adjunto, como archivos .pdf o .zip.

Por eso es importante nunca hacer clic en un enlace de un correo electrónico sospechoso y nunca abrir un archivo adjunto de un correo electrónico sospechoso. El malware puede adoptar muchas formas: virus, gusanos, botnets y ransomware.

Virus

Los virus son un subgrupo del malware. Un virus es un software malicioso adjunto a un documento o archivo que admite macros para ejecutar su código y transmitirse de un sistema a otro. Una vez descargado, el virus permanece inactivo hasta que el archivo se abre y se utiliza. Los virus están diseñados para perturbar la capacidad de funcionamiento de un sistema. Como resultado, los virus pueden causar importantes problemas operativos y pérdida de datos.

Gusanos

Un gusano es un tipo de software malicioso que se replica rápidamente y se extiende a cualquier dispositivo de la red. A diferencia de los virus, los gusanos no necesitan programas anfitriones para transmitirse. Un gusano infecta un dispositivo a través de un archivo descargado o una conexión de red antes de multiplicarse y extenderse a un ritmo exponencial. Al igual que los virus, los gusanos pueden perturbar gravemente el funcionamiento de un dispositivo y provocar la pérdida de datos.

Adware

El adware es un programa malicioso que se utiliza para obtener datos sobre el uso de su computadora y ofrecerle anuncios publicitarios apropiados. Aunque el adware no siempre es peligroso, en algunos casos puede causar problemas en el sistema. El adware puede redirigir su navegador a sitios no seguros, e incluso puede contener troyanos y spyware. Además, niveles significativos de adware pueden reducir notablemente la velocidad de su sistema. Dado que no todo el adware es malicioso, es importante contar con una protección que analice estos programas de forma constante e inteligente.

Virus troyano

Los virus troyanos se disfrazan de programas útiles. Pero una vez que el usuario lo descarga, el virus troyano puede acceder a datos confidenciales y luego modificarlos, bloquearlos o borrarlos. Esto puede ser extremadamente peligroso para el funcionamiento del dispositivo. A diferencia de los virus y gusanos normales, los virus troyanos no están diseñados para autorreplicarse.

Spyware

El spyware es un programa malicioso que se ejecuta en secreto en una computadora e informa a un usuario remoto. En lugar de limitarse a interrumpir el funcionamiento de un dispositivo, el spyware se dirige a la información sensible y puede conceder acceso remoto a los estafadores. Los programas espía suelen utilizarse para robar información financiera o personal. Un tipo específico de spyware es el keylogger, que registra las acciones del usuario para revelar contraseñas e información personal.

Ransomware

El ransomware es un programa malicioso que accede a información confidencial de un sistema, la encripta para que el usuario no pueda acceder a la información, y luego exige un pago económico para liberar los datos. El ransomware suele formar parte de una estafa de phishing. Al hacer clic en un enlace engañoso, el usuario descarga el ransomware. El estafador procede a encriptar información específica que sólo puede abrirse mediante una clave matemática que él conoce. Cuando el estafador recibe el pago, los datos se desbloquean.

Malware sin archivos

El malware sin archivos es un tipo de malware residente en memoria. Como sugiere el término, se trata de malware que opera desde la memoria de la computadora de la víctima, no desde archivos en el disco duro. Como no hay archivos que escanear, es más difícil de detectar que el malware tradicional. También dificulta el análisis forense porque el malware desaparece cuando se reinicia la computadora de la víctima.

Consejo sobre phishing #2

Las empresas legítimas suelen utilizar el nombre de su empresa como nombre de dominio. Si usted está recibiendo un correo electrónico de aspecto oficial de una cuenta pública (yahoo, gmail, outlook, hotmail, etc.) o de una cuenta con un montón de números extraños, lo más probable es que sea una estafa.

Siempre revise la dirección de correo electrónico para ver si coincide con el nombre de la cuenta. Y, si es posible, revise la dirección de respuesta. Las empresas legítimas no le pedirán que les envíe información privada por correo electrónico. Acceda a su cuenta en la web y compruebe si los mismos mensajes aparecen en su cuenta.

También puede llamar a la empresa para ver si tienen dudas o preguntas legítimas.

Pero, ¿cómo consiguieron esos estafadores mi dirección de correo electrónico?

Los estafadores pueden haber obtenido su dirección de correo electrónico de varias formas:

- **Búsqueda en registros públicos.** A los estafadores les resulta muy fácil encontrar su dirección de correo electrónico si alguna vez la ha publicado en el internet.
- **Adivinar.** Los estafadores suelen probar combinaciones de correo electrónico comunes, como nombre.apellido, hasta que obtienen un resultado correcto.
- **Compra de listas de correo electrónico**. Un estafador puede haber comprado una lista de direcciones de correo electrónico (legal o ilegalmente) que contenga su dirección.
- **Una violación de datos.** Los estafadores pueden haber encontrado su dirección de correo electrónico tras una infiltración de datos.
- **Rastreo de redes sociales.** Es muy fácil rastrear sitios como LinkedIn para obtener su información de contacto personal.
- **Surfeo de hombro.** Los estafadores observarán cómo usted introduce su dirección de correo electrónico en público y la añadirán a su lista de spam.

¿Pueden ver los estafadores que he abierto su correo electrónico?

Depende. Los estafadores podrán saber que usted abrió un correo electrónico si descarga algún archivo adjunto o hace clic en algún enlace (algo que NUNCA debe hacer), o si su servicio de correo electrónico carga automáticamente las imágenes incluidas en el mensaje.

Si esto último le ha sorprendido, es cierto: los estafadores pueden obtener un montón de datos sobre usted si tiene activada la carga automática de imágenes. Si tiene activada la carga automática de imágenes, los estafadores pueden ver:

- Su ubicación
- Su proveedor de servicios de Internet o de servicios de teléfono celular
- El dispositivo que usted utilizó para abrir el correo electrónico (computadora de escritorio, laptop, tableta, iPhone/Android)
- El sistema operativo que usted está utilizando (iOS, Mac, Android, Microsoft Windows, Linux)
- El servicio de correo electrónico que usted utiliza (Apple Mail, Outlook, Gmail o Yahoo Mail).
- El navegador web que usted está utilizando (Apple Safari, Google Chrome o Firefox)

Conclusión clave: Desactive la carga automática de imágenes. La mayoría de los servicios de correo electrónico le permitirán desactivar la carga automática de imágenes en la configuración de su cuenta de correo electrónico.