Título: Consejos para Mantenerse Seguro en Línea: Cómo Identificar Correos Electrónicos de Phishing

Presentación: La Serie de Videos Consejos para Mantenerse Seguro en Línea se organiza mediante diapositivas como marcadores visuales. Cualquier imagen de las diapositivas que sea importante para el contenido, y exprese cualquier información adicional más allá del guion, se incluye aquí como texto alternativo.

Narrador: Bienvenidos al video de Help@Hand Cómo Identificar Correos Electrónicos de Phishing. Help@Hand es una Colaboración de múltiples ciudades y condados creada para ayudar a dar forma al futuro de soluciones de salud mental basadas en la tecnología y conectar a las personas con los cuidados por todo el estado. La intención de estos tutoriales en video es empoderar a las comunidades de California para que tomen decisiones informadas sobre la forma en que interactúan con la tecnología. Este es el curso [3] de una serie de 4 cursos llamada Consejos para Mantenerse Seguro en Línea. Los videos de esta serie pueden verse por orden, o en cualquier orden según sus intereses.

Narrador: Muchos correos electrónicos son inofensivos, pero algunos correos electrónicos que recibimos pueden ser enviados por extraños que están intentando acceder a nuestros datos personales y financieros. El tutorial que sigue le ayudará a entender qué son los correos electrónicos de phishing y cómo puede identificarlos

Narrador: Los correos electrónicos de phishing pueden parecer reales, pero a menudo tienen enlaces o adjuntos que pueden ser dañinos cuando hacemos clic en ellos. (clic) El propósito de estos correos es conseguir acceso a los datos de usted o hacer que usted descargue accidentalmente malware y virus que pueden dañar su computadora y dejar aún más expuestos sus datos. Afortunadamente, hay algunas pistas que usted puede buscar para ayudarle a identificar un correo electrónico de phishing.

Imagen: Se muestra un correo en una ventana emergente. Hay un nombre de remitente del correo que dice joykone y una dirección de correo que dice konemrskone10@gmail.com. A la izquierda del nombre del remitente del correo hay un círculo con un octágono en el centro y una “X”. Bajo el nombre y la dirección de correo del remitente hay un recuadro rojo que dice “Este mensaje parece peligroso. Se han usado mensajes similares para robar información personal de las personas. Evite hacer clic en enlaces, descargar adjuntos, o contestar con información personal.” También hay un recuadro en el que se puede hacer clic que dice “Parece seguro”. El texto del correo electrónico dice “De la Sra. Joy Kone, Estimado, quiero pedir su ayuda. Mi nombre es Sra. Joy Kone, soy viuda. Mi esposo y yo trabajamos para Tullow oil hasta que él murió hace siete años. Estoy interesada en que usted sea mi socio para inversiones extranjeras para transferir un depósito de $18,300,000.00 USD a su país.

Narrador: El primer consejo es mirar la persona o compañía que envió el mensaje. ¿Usted la conoce, y la dirección de correo de esa persona está escrita correctamente? Una vez haya decidido esto, lea cuidadosamente la línea del asunto del mensaje y el propio mensaje para ver si hay alguna señal de peligro. Si hay muchos errores de ortografía o gramática, o sencillamente no suena como la persona que lo ha enviado, asegúrese

de no hacer clic en ninguno de los enlaces o adjuntos que puedan aparecer en el mensaje. En este correo electrónico de ejemplo, el remitente del mensaje, la "Sra. Joy Kone" no es conocida para la persona que recibe el correo electrónico. El propio mensaje también es bastante sospechoso. ¿Por qué compartiría la Sra. Kone este tipo de información personal con alguien que no conoce, y también iba a ofrecerse a transferir una cantidad tan grande de dinero?

Imagen: Se muestra un correo electrónico. La línea de asunto dice "Fwd: Para todos", con un emoticono de una cara sonriente. El nombre y dirección de correo del remitente dicen "Michelle Vega lukaslogo@yandex.ru" el mensaje dice "Creo que usted puede encontrar esto interesante http://ub2l.ugtssxw.info/'

Narrador: Este es otro ejemplo de correo electrónico en el que el remitente del correo realmente es conocido para la persona que recibe el mensaje. Sin embargo, cuando se mira más de cerca, la dirección de correo no está asociada con su persona, y el texto del mensaje parece raro porque contiene un enlace sin ninguna otra información que lo explique. En este caso, no sería buena idea hacer clic en el enlace y arriesgarse a exponerse a extraños que podrían robar sus datos. La mejor estrategia sería redactar un mensaje por separado a Michelle para averiguar si ella le envió a usted el mensaje. Si no, es posible que la computadora de Michelle haya estado expuesta a un virus que está enviando correos electrónicos de phishing a sus contactos. Si es así, es especialmente importante que usted no haga clic en ningún enlace o adjunto, y que no reenvíe el correo electrónico a otras personas. Hacer esto podría extender más el virus y hacer a otras personas vulnerables al ataque de phishing.

Imagen: Se ve un correo electrónico en una ventana que se abre. La línea de asunto dice "¡Solicite Un Préstamo Hoy! Hasta $35k", a continuación el nombre y dirección del correo del remitente dicen "ChristmasCashNow <offer.chcf43264@cf607ntnv1rkk4.w1e5-aa8e.uclgk7w.gq." A la izquierda del nombre del remitente del correo hay un círculo con un octágono en el centro y el signo "!". Bajo el nombre y dirección de correo del remitente hay un recuadro que dice "¿Por qué está este mensaje en spam? Es parecido a correos que se identificaron como spam en el pasado. También hay un recuadro en el que se puede hacer clic que dice "Reportar como no spam". El mensaje del correo dice "Solicite un préstamo. Con ChristmasCashFast, usted puede recibir financiación hasta $35,000. Somos socios de más de 100 prestamistas autorizados. Esto nos permite cubrir casi 50 estados. Los $35,00 se reciben rápidamente y desde la privacidad de su propio hogar. ¡Consiga fondos para Navidad! Préstamos personales rápidos en línea. Todos los tipos de créditos son bienvenidos, los fondos depositados directamente. ¡Empiece Ya!". La prueba "¡Empiece Ya!" está en un recuadro en el que se puede hacer clic.

Narrador: Esto nos lleva al consejo número dos. Cuando esté leyendo un correo, debe pensar siempre con cuidado en lo que le está diciendo el mensaje. Una cosa que debe preguntarse es: "¿Es demasiado bueno para ser verdad?" Muchos correos electrónicos de phishing contienen notificaciones sobre ganar grandes premios o acceder a servicios de citas dudosos. Por ejemplo, este correo hace que casi sea demasiado fácil solicitar un préstamo. También es sospechoso que se ofrezcan a depositar los fondos directamente en la cuenta de esta persona, ya que necesitarían

todos los datos personales de la cuenta para hacerlo. Una vez más, si tiene dudas sobre un correo electrónico, es muy importante que NO haga clic en ninguno de los enlaces del mensaje.

Imagen: Se muestra un correo en una ventana emergente con un logo de eBay en la parte superior. El nombre y dirección de correo del remitente dice “Departamento de Seguridad de Cuentas de eBay”, la línea del asunto dice “Se necesita cambio de contraseña” el mensaje del correo dice “¡Se necesita cambio de contraseña! Estimado señor, hemos determinado que distintas computadoras se han conectado a su cuenta de eBay, y estuvieron presentes múltiples fallos de contraseña antes de las conexiones. Le aconsejamos encarecidamente que CAMBIE SU CONTRASEÑA. Si esto no se completa para el 8 de marzo de 2007, nos veremos obligados a suspender indefinidamente su cuenta, puesto que puede haber sido usada para fines fraudulentos. Gracias por su cooperación. Haga clic aquí para Cambiar Su Contraseña. Gracias por su pronta atención a este asunto. Sentimos cualquier molestia. ¡Gracias por usar eBay! Por favor, no conteste este correo. Los correos enviados a esta dirección no pueden responderse.’

Narrador: Otros correos electrónicos falsos utilizan técnicas para causar miedo para engañar a la gente y que haga clic en enlaces o contesten al mensaje con datos personales. Estos correos electrónicos a menudo parecerán urgentes y suelen contener un aviso de que sucederá algo malo si el destinatario del correo no actúa rápidamente. En este mensaje se le dice a la persona que tiene un plazo para hacer el cambio de contraseña, o de lo contrario se suspenderá su cuenta. Cuando reciba un correo electrónico que le pida que cambie su contraseña, en lugar de hacer clic en el enlace, normalmente es buena idea ir a su navegador, escribir la dirección del sitio del que viene el correo, asegurarse de que es el sitio auténtico, y hacer cualquier cambio directamente a través del sitio. En este caso, la persona debe ir directamente a su cuenta de eBay para ver si necesita actualizar su contraseña. Si el sitio auténtico de eBay no menciona que debe cambiar su contraseña, entonces es probable que este mensaje de correo electrónico sea falso.

Imagen: Se muestra un correo electrónico, la línea de asunto en la parte superior dice “Consiga un nuevo Especial de Alarma + $100 de Bonificación en Tarjeta Visa de Proteja Su Hogar” debajo hay un marcador de la plataforma de correo electrónico que etiqueta el mensaje como spam. El nombre y correo del remitente dice “Protect Your Home adtm43275@tl6ofeogvqj8b.wfcc-9101.gm8xuiii.ga” Bajo el nombre y dirección de correo del remitente hay un recuadro que dice “¿Por qué está este mensaje en spam? Es parecido a correos que se identificaron como spam en el pasado. También hay un recuadro en el que se puede hacer clic que dice “Reportar como no spam.” El mensaje del correo electrónico dice “¿Cuál es su plan para ayudar a proteger su familia hogar? “¡El 87% de todos los Robos en Hogares se Consideran Evitables!* Sabía Usted: El costo medio de los daños por intrusión en un hogar es de $1000. Según el FBI, se produce un robo en casas en algún lugar de los EE.UU. cada 15.4 segundos. ¡No sea un blanco fácil!.” En la parte inferior del mensaje hay un recuadro en el que se puede hacer clic que dice “PRUEBA GRATUITA.”

Narrador: En este correo, el remitente está intentando asustar a la persona para que haga clic en el correo dando estadísticas sobre estadísticas de robos en hogares y haciendo

que la persona se sienta presionada para actuar rápidamente para protegerse a sí misma y a su familia.

Imagen: Se muestra un correo electrónico, la línea de texto dice “responda urgente” bajo esto hay un marcador de la plataforma de correo que etiqueta el correo como spam. El nombre y correo del remitente dice “ Shahinaz Zuthimalin fulltime343@yahoo.com.” A la izquierda del nombre del remitente del correo hay un círculo con un octágono en el centro y una “X”. Bajo el nombre y la dirección de correo del remitente hay un recuadro rojo que dice “Este mensaje parece peligroso. Se han usado mensajes similares para robar información personal de las personas. Evite hacer clic en enlaces, descargar adjuntos, o contestar con información personal.” También hay un recuadro en el que se puede hacer clic que dice “Parece seguro”. El mensaje del correo dice “Hola, Estimado, Por favor no se sienta molestado porque le haya contactado, basándome en la condición crítica en la que me encuentro, sin embargo, no es problema financiero, pero mi salud usted puede haber saber que el cáncer no es algo para hablar en casa, estoy casada con el Sr. Khalil Zuthimalin que trabajó para la embajada de Túnez en Burkina Faso durante nueve años hasta su muerte en el año 2012. Estuvimos casados once años sin hijos. El murió después de una breve enfermedad que duró cinco días. Desde su muerte decidí no volverme a casar, Cuando mi difunto marido estaba vivo depositó la cantidad de US $ 9.2m (Nueve millones doscientos mil dólares) en un banco en Burkina Faso, Actualmente este dinero está aún en un banco. Y mi Médico me dijo que no tengo mucho tiempo para vivir por el problema de cáncer, Habiendo conocido mi condición decidí entregarle a usted este fondo para cuidar de las personas menos privilegiadas, usted.”

Narrador: Un tercer consejo es prestar atención a la forma en que su proveedor de correo electrónico etiqueta estos mensajes entrantes. Su cuenta de correo electrónico tiene ajustes para filtrar automáticamente mensajes peligrosos que podrían ser dañinos para usted. Si un correo electrónico se etiqueta como “spam”, usted debe actuar con cautela. SI un correo tiene una alerta, lo más seguro es borrar el mensaje. Este correo tiene una alerta que dice al destinatario de correo que no haga clic en enlaces, no descargue adjuntos, ni conteste con ningún tipo de información personal. Esto tiene sentido, ya que el correo tiene un mensaje urgente de una persona desconocida en la que probablemente no se debería confiar.

Narrador: Así pues, recapitulemos: recuerde estos consejos cuando esté decidiendo si confía o no en un mensaje de correo electrónico.

a. Consejo 1. Piense en el remitente. ¿Lo conoce? ¿Hay errores de ortografía? ¿Parece sospechoso?
b. Consejo 2. Piense en lo que está diciendo el mensaje y si su proveedor de correo electrónico piensa que es seguro o no. ¿Es demasiado bueno para ser verdad? ¿Hay una sensación de urgencia?
c. Consejo 3. Si su proveedor de correo piensa que es peligroso, probablemente lo es. ¿Llegó su correo con algún anuncio de virus o spam?

Narrador: Esperamos que haya encontrado útil este video. A pesar de que es opcional, le rogamos que, por favor, dedique un minuto a proporcionar retroinformación sobre

su experiencia, haciendo clic en el enlace de encuesta que aparecerá en breve. Gracias por participar, y no olvide ver los demás videos de Help@Hand.