Taller de capacitación sobre conceptos básicos de ciberseguridad

Reseña del instructor: La ciberseguridad

Este documento está diseñado para que el instructor lo utilice junto con la presentación de PowerPoint y/o la demostración en vivo. Incluye una descripción general del curso, puntos de conversación e instrucciones para las actividades. Tenga en cuenta las anotaciones del número de la diapositiva para que le ayuden a conservar el rumbo.

Descripción del taller

Este taller virtual o en persona es para aquellos que están interesados en la seguridad en línea y quieren protegerse de los estafadores y las estafas. Desarrollará la confianza de los asistentes cuando visiten sitios web, creen contraseñas y respondan correos electrónicos.

Trayectoria del plan de estudios

Conceptos básicos

Audiencia

Personas adultas de viviendas recientemente conectadas y/o que están buscando desarrollar habilidades básicas y confianza en el uso de la tecnología.

Duración del taller

De 60 a 90 minutos

Método de entrenamiento

Práctica dirigida por un instructor voluntario

Objetivo

En este taller, usted les presentará a los usuarios de computadoras e Internet recién conectados la seguridad básica cuando visitan sitios web, crean contraseñas y reciben correos electrónicos y otras comunicaciones de posibles estafadores. Un objetivo principal del taller es que los alumnos aumenten la confianza en su capacidad para participar en línea mientras se mantienen protegidos de estafas y

fraudes.

Requisitos de equipamiento

En persona: Proyector y pantalla de proyección; computadoras para el instructor y los participantes con conexión a Internet; puntero láser (recomendado).

Solo para el entorno del salón de clases (con participantes que no tienen computadoras), el instructor proyectará una demostración en vivo e involucrará a los participantes hablando sobre las actividades y realizando tareas interactivas en un formato de debate en grupo.

Virtual: Una plataforma de conferencias web, computadoras para el instructor y los participantes con conexión a internet.

Requisitos de software

Una computadora capaz de ejecutar una presentación de PowerPoint con un explorador web, preferiblemente Google Chrome.

Requisitos de materiales

- Hojas de papel, bolígrafos o lápices
- Presentación de PowerPoint del instructor: Antes del taller, revise las diapositivas y actualice la siguiente información:
    - Verifique el explorador web que usará durante el taller y cómo iniciar el explorador desde el escritorio.
    - Diapositiva 1: Actualice el nombre del instructor, la afiliación del instructor (por ejemplo, miembro del personal de la biblioteca, voluntario de la comunidad, etc.) y el nombre de la ubicación. Inserte la URL de la biblioteca. Esté preparado para dar una breve introducción sobre usted.
    - Diapositiva 56: Inserte el nombre y la fecha del próximo taller, si es que se ofrece.
- Reseña del instructor (este documento): Revise la reseña del instructor y familiarícese con los materiales del taller.
- Folleto del alumno
    - Para el taller en persona: Imprima el folleto para cada asistente y entréguelos a los alumnos antes de que comience el taller.
    - Para el taller virtual: Proporcione un enlace al folleto del alumno antes del taller como parte de la confirmación de su registro o inclúyalo en la función de chat de la plataforma en línea.
- Hoja de actividades del alumno
    - Para el taller en persona: Imprima el folleto para cada asistente y entréguelos antes de que comience el taller.

    - Para el taller virtual: Haga las preguntas enumeradas en la Hoja de actividades durante el taller y pida a los asistentes que compartan su respuesta a través del chat o use la herramienta de encuesta interna, si está disponible dentro de la herramienta de conferencia web.
- Certificado de finalización: Para el taller en persona, imprima los certificados para entregar a cada asistente una vez finalizado el taller. Para los asistentes virtuales, envíeles una copia electrónica por correo electrónico.
- Etiquetas de nombre de los asistentes: Si desea identificar fácilmente a los asistentes, asegúrese de traer etiquetas adhesivas o tarjetas para la mesa con sus nombres.

Objetivos de aprendizaje

Al final de la sesión, los alumnos podrán:

- Identificar un sitio web seguro (es decir, un sitio web en el que es seguro crear una cuenta).
- Utilizar dos consejos del taller para crear una contraseña segura que sea fácil de recordar.
- Identificar los factores clave en un mensaje de correo electrónico que indican que se trata de una estafa.

Antes de que comience el taller

- En persona:
    - Asegúrese de que todas las computadoras estén encendidas y listas para que las utilicen los asistentes. (Consulte la nota anterior sobre la configuración del salón, en la sección "Requisitos de equipamiento").
    - Coloque los materiales de los asistentes en cada computadora. Los materiales para los asistentes incluyen la Hoja de actividades del alumno y el Folleto del alumno. También puede proporcionar papel (para que los asistentes tomen notas) y un bolígrafo o lápiz.
    - Si usa etiquetas para los nombres, asegúrese de que los asistentes puedan acceder fácilmente a ellas y proporcione un marcador o bolígrafo para que los asistentes escriban su nombre.
    - Mantenga una lista de inscripción para que pueda identificar a los que asistieron.
    - Revise la computadora antes del curso y vea qué explorador web está instalado y cómo iniciarlo desde la computadora.
    - Determine un “lugar de estacionamiento" para darle seguimiento a las preguntas que se responderán más adelante en el taller. Algunos lugares sugeridos para un "lugar de estacionamiento" son una pizarra, un rotafolio o un bloc de notas. Aliente a los alumnos a que tomen nota del número de la diapositiva y la sección a medida que “estacionan” las preguntas.
- Virtual:
    - Envíe instrucciones a los participantes sobre cómo conectarse al taller. Si es posible, podría crear un video o documento corto con instrucciones paso a paso (con imágenes) para proporcionar una descripción general básica de cómo usar la herramienta de conferencias web para compartir con sus participantes.

- Envíe un enlace antes del taller a los materiales del alumno. Estos incluyen la Hoja de actividades del alumno y el Folleto del alumno. Durante el taller, vuelva a enviar el enlace a través de la herramienta de chat de la conferencia web.
- Mantenga una lista de inscripción para que pueda identificar a los que asistieron.
- Determine un “lugar de estacionamiento" que es un lugar para que los participantes hagan preguntas y una forma para usted de darle seguimiento fácilmente a las preguntas que se responderán más adelante en el taller. Para su estacionamiento virtual, es posible que desee utilizar la función de chat o la función de preguntas de la herramienta de conferencia web. Aliente a los alumnos a que tomen nota del número de la diapositiva y la sección a medida que “estacionan” las preguntas.

Técnica(s) de evaluación

Finalización exitosa de actividades

Diapositiva 1: Conceptos básicos de ciberseguridad. Muestre la diapositiva del título del taller.

Actualice esta diapositiva con la información apropiada:

- *Nombre del instructor*
- *Afiliación del instructor (por ejemplo, miembro del personal de la biblioteca, voluntario de la comunidad, etc.)*
- *Nombre del lugar*

Antes del taller, revise la reseña del instructor. Esto le proporciona orientación sobre cómo prepararse y llevar a cabo el taller y detalles sobre lo que debe hacer una vez que termine el taller.

NOTA AL INSTRUCTOR: Incluya un agradecimiento al colaborador de la comunidad, si corresponde

Me llamo **<escriba su nombre aquí>** y soy **<breve descripción de sí mismo>**. Antes de comenzar, aquí hay algunos elementos de gestión administrativa que deben conocer: (mencione los elementos que son relevantes para su taller)

- ¿Dónde están los baños?
- ¿Dónde están las salidas de emergencia?
- Cuándo/cómo hacer las preguntas. Señale el número de página que se encuentra en cada diapositiva para que los participantes lo escriban junto con la pregunta que hagan.
- Si tiene un teléfono celular con usted, asegúrese de apagarlo o ponerlo en silencio.
- ¿Habrá un descanso?

Diapositiva 2: Reseña del contenido del taller - Agenda (3 minutos)

En este taller, aprenderá sobre la ciberseguridad, en otras palabras, cómo mantener sus cuentas e identidad seguras en línea. Trabajaremos en desarrollar las habilidades y la confianza para mantener su seguridad. Se incluirá lo siguiente:

- Reconocer los sitios web seguros
- Crear contraseñas seguras y fáciles de recordar para sus cuentas, y
- Reconocer las estafas communes

A medida que avanzamos, aprenderá **Consejos y trucos** para tener contraseñas seguras y evitar las estafas. Además, tendrá oportunidades para practicar lo que ha aprendido.

¡Empecemos!

Diapositiva 3: ¿Por qué debemos preocuparnos por la seguridad cuando estamos en línea?

NOTA AL INSTRUCTOR: Pida a los asistentes que respondan la pregunta que aparece en la diapositiva. Dirija un breve debate sobre la seguridad y, luego, continúe con la información. O bien, puede hacer la pregunta, esperar un momento para que los asistentes piensen en ella y continuar con la información.

Presione Enter (Intro) para la viñeta 1:

Cuando navegamos por la web, creamos cuentas personales en sitios web y usamos el correo electrónico, compartimos información personal que queremos mantener privada. Esto incluye la información de tarjetas de crédito, información bancaria, información de salud personal y más. Necesitamos mantener esta información segura y privada.

Presione Enter (Intro) para la viñeta 2:

Desafortunadamente, los estafadores a veces intentarán obtener acceso a esta información. Es posible que intenten obtener acceso a sus cuentas personales adivinando sus contraseñas, consiguiendo que usted les envíe información o persuadiéndolo para que instale un software en su computadora o dispositivo que les permita acceder a su información.

Diapositiva 4: ¿Qué es la ciberseguridad?
La ciberseguridad tiene que ver con la seguridad de la información (nuestra identidad, nuestros datos personales y nuestros activos financieros) cuando estamos en línea.

Para personas como usted y yo, la ciberseguridad significa que 1) sus datos personales son accesibles solo para usted u otras personas que usted autorice, y 2) sus dispositivos (computadoras portátiles, computadoras de escritorio, teléfonos móviles, tabletas) funcionan correctamente y no tienen malware. El malware es un software malicioso que puede tomar muchas formas: desde virus que infectan sus dispositivos favoritos hasta spyware y adware que rastrean sus actividades en línea.

Diapositiva 5: Sitios web seguros.

Comencemos hablando de los sitios web seguros. ¿Por qué un sitio web debe ser seguro? Si va a ingresar información personal en un sitio web, desea mantener su información segura.

NOTA AL INSTRUCTOR: Haga la pregunta de la diapositiva a los asistentes, pídales que compartan sus ideas y, luego, continúe con la viñeta. O bien, puede hacer la pregunta, esperar un momento para que los asistentes piensen en ella y continuar con la información.

Diapositiva 6: Sitios web seguros. Hay dos cosas que debe buscar cuando visita un sitio web:

1) un ícono de candado junto a la barra de direcciones, y

2) una dirección de sitio web que comience con HTTPS.

Presione ENTER (Intro) para agrandar la imagen y el símbolo:

Si el sitio web tiene uno o ambos, el sitio web es seguro. Eso significa que es seguro explorar sin ser rastreado, y que es seguro crear una cuenta y compartir la información personal.

En muchos navegadores modernos, es posible que la dirección del sitio web no muestre el comienzo de la URL a menos que haga doble clic en la dirección. Recuerde, si no puede ver el HTTPS, asegúrese de poder ver el ícono del candado.

Diapositiva 7: Sitios web seguros. Si el sitio web no tiene un ícono de candado, no es seguro. Si la dirección del sitio web no comienza con HTTPS, sino con HTTP sin la S, el sitio no es seguro.

Presione ENTER (Intro) para agrandar la imagen y el símbolo

La mayoría de los navegadores modernos muestran algún tipo de advertencia para ayudarle a determinar si el sitio es seguro. En este ejemplo, el navegador muestra un signo de exclamación para llamar su atención. Si no ve el candado, use un sitio web diferente si es posible.

Diapositiva 8: Cuentas personales.

NOTA AL INSTRUCTOR: Facilite un breve debate con los asistentes. ¿Han creado una cuenta en línea? ¿Qué tipos de cuentas han creado? ¿Por qué alguien crearía una cuenta en un sitio web?

Posibles tipos de cuentas sobre las que los asistentes pueden debatir: correo electrónico, redes sociales, sitios de búsqueda de empleo, escuelas, bancos y tarjetas de crédito, plataformas de medios y noticias, sitios de transmisión de video y sitios de ventas minoristas.

Una cuenta personal es esencial para servicios como el correo electrónico, donde desea tener su propia cuenta que sea privada para usted. Muchos sitios web y aplicaciones ofrecen o, a veces, requieren una cuenta personal para usarlos.

Una de las razones principales para crear una cuenta personal es poder realizar un seguimiento de lo que hace en un sitio web o una aplicación, como ver transmisiones de video, solicitar empleos, realizar un seguimiento de las compras y mucho más. Algunos contenidos de los sitios web están disponibles solo si ha iniciado sesión en su cuenta. Con una cuenta en línea, puede pagar facturas, como las de los teléfonos, el alquiler o la hipoteca, y los servicios públicos. Una cuenta en línea es fundamental para las cuentas bancarias y otras cuentas financieras. ¿Por qué? Para que solo usted pueda acceder a ellas.

Presione Enter (Intro) para la viñeta 1

Usted crea una cuenta personal para que su información sea **accesible solo para usted.**

Diapositiva 9: Sitios web seguros.

NOTA AL INSTRUCTOR: Vincule la información de las cuentas personales con la importancia de los sitios web seguros. Reitere la información sobre los sitios web seguros.

Esta es la razón por la que los sitios web seguros son importantes: para que sus datos estén protegidos. Es importante mantener su cuenta segura en cualquier sitio web. Si alguien obtiene acceso a una de sus cuentas en línea, su información personal también podría usarse para acceder a otras cuentas. O su cuenta podría incluso ser utilizada por piratas informáticos e impostores para cometer delitos.

NOTA AL INSTRUCTOR: Antes de pasar a la Actividad 1, revise las preguntas del "lugar de estacionamiento". Si no hay preguntas en el "lugar de estacionamiento", averigüe con los asistentes si tienen alguna pregunta antes de pasar a la Actividad 1.

Diapositiva 10: Actividad 1 — Sitios web seguros.

NOTA AL INSTRUCTOR: Dirija a los asistentes a la Actividad 1 en la página 1 de la Hoja de actividades.

Si los alumnos están usando computadoras, anímelos a seleccionar un sitio web que podrían usar para las compras, operaciones bancarias, redes sociales, etc. Los asistentes van al sitio web y completan las preguntas de la actividad. Facilite un breve debate. ¿Qué sitios web visitaron? ¿Eran sitios web seguros? ¿Cómo lo pueden saber?

Si no hay computadoras, pida a los asistentes que mencionen algunos sitios web que podrían visitar para las compras, operaciones bancarias, redes sociales, etc. Vaya a los sitios web que mencionan y pida a los asistentes que compartan cómo pueden saber que es seguro. Facilite un breve debate.

Diapositiva 11: Informe de la Actividad 1.

NOTA AL INSTRUCTOR: Use la diapositiva para informar sobre la actividad o como guía para usted mismo si está haciendo una demostración.

Sitios seguros sugeridos para el instructor para hacer una demostración:

- *https://www.digitallearn.org*
- *google.com*
- *nypl.org*

Respuestas a las preguntas:

1. Ícono de candado – *instructor: señale el candado en su ejemplo.*

2. https:// visible en la barra de direcciones o si hace doble clic en la barra de direcciones *(instructor — haga una demostración si https:// no está visible.*

Diapositiva 12: Contraseñas seguras.

Cuando creamos cuentas personales en sitios web, es importante asegurarnos de que las contraseñas de nuestras cuentas sean lo más seguras posible.

Continuemos nuestro debate sobre la seguridad en línea con un vistazo a las contraseñas seguras. Cuando creamos cuentas personales en sitios web, es importante asegurarnos de que las contraseñas de nuestras cuentas sean lo más seguras posible.

Diapositiva 13: Contraseñas seguras.

NOTA AL INSTRUCTOR: Facilite un breve debate con los asistentes. "¿Cómo inventan una contraseña? ¿Cómo hacen que sea fuerte y segura?"

NOTA AL INSTRUCTOR: Es importante basarse en las fortalezas y no avergonzar a los asistentes por los enfoques que utilicen.

¡Buenas respuestas! Aprendamos más sobre cómo podemos crear contraseñas seguras.

Diapositiva 14: Contraseñas seguras.

La mayoría de los sitios web tienen requisitos para las contraseñas en sus formularios de registro. Los requisitos generalmente se enumeran debajo del formulario. Es posible que los requisitos no se muestren hasta que su contraseña no incluya los requisitos.

Presione ENTER (Intro) para la lista de viñetas:

Las contraseñas usualmente pueden incluir números, letras mayúsculas y minúsculas, y símbolos como puntuación. Si no se acepta su primer intento, revise los requisitos del sitio web. Luego, intente agregar una letra mayúscula, un número o un símbolo, o haga que la contraseña sea más larga.

En este caso, la contraseña debe tener cuando menos ocho caracteres y contener al menos una letra mayúscula, una letra minúscula y un número.

Diapositiva 15: Consejos para contraseñas seguras.

¿Cómo sería una contraseña segura? Estas son algunas de las cosas que debe y no debe hacer.

Presione ENTER (Intro) para la viñeta 1 Evite las contraseñas débiles, como "contraseña" (¡que es la contraseña que se usa más comúnmente!) o "123456".

Presione ENTER (Intro) para la viñeta 2 No incluya información personal, como su dirección o nombre.

Presione ENTER (Intro) para la viñeta 3 No use la misma contraseña en varios sitios web o varias cuentas.

Presione ENTER (Intro) para la viñeta 4 No comparta su contraseña con otros. Las contraseñas son la llave secreta que abre su cuenta. Deben mantenerse privadas.

Diapositiva 16: Consejos para contraseñas seguras

Haga la contraseña más larga. La mejor defensa es la longitud.

Presione Enter (Intro) para la imagen:

Las contraseñas largas no necesitan ser complejas y difíciles de recordar. Es posible que estemos acostumbrados a crear contraseñas largas y complicadas que son difíciles de recordar.

Presione Enter (Intro) para la viñeta 2:

Pero podemos crear una contraseña larga y segura que sea más fácil de recordar usando frases cortas. Un ejemplo podría ser "Vacasayudanahacerqueso".

Recuerde, muchos sitios web tienen requisitos para las contraseñas. Estos requisitos generalmente se enumeran debajo del campo de contraseña o se identifican una vez que hace clic en el campo de contraseña. Es posible que le soliciten que incluya letras mayúsculas y minúsculas, números y símbolos.

Diapositiva 17: Lleve un registro de sus contraseñas

NOTA AL INSTRUCTOR: ¿Cómo recuerdan sus contraseñas? Facilite un breve debate.

Es importante basarse en las fortalezas y no avergonzar a nadie. Es posible que parte de este debate ya haya aparecido en la sección Contraseñas seguras. Los comentarios anteriores de los asistentes pueden incluirse aquí si corresponde.

Ahora que hemos discutido la creación de una contraseña segura, hablemos sobre cómo podemos llevar un seguimiento de nuestras contraseñas.

Si ha usado Internet durante un tiempo, puede que haya creado muchas cuentas en muchos sitios web o aplicaciones móviles. Sus contraseñas pueden ser diferentes en cada sitio, y es más seguro si lo son, por lo que puede ser un reto recordarlas.

Presione Enter (Intro) para la lista numerada:

Veamos algunos enfoques diferentes que podríamos tomar para recordar nuestras contraseñas.

Diapositiva 18: Elemento 1: Cuaderno.

Puede optar por escribir sus contraseñas en un cuaderno. Si hace esto, asegúrese de guardar el cuaderno en un lugar seguro y protegido.

Presione ENTER (Intro) para los consejos:

En lugar de escribir la contraseña real, escriba algo que le ayude a recordar la contraseña real.

Diapositiva 19: Elemento 2: Software de contraseñas.

También puede optar por usar una aplicación móvil o un sitio web seguro para administrar contraseñas que puede ayudarle a llevar un registro de las contraseñas. Estos programas generalmente se desbloquean con una sola contraseña maestra y luego le permiten acceder a todas sus contraseñas cuando las necesita. Las aplicaciones también generan contraseñas para usted que son combinaciones complejas de letras, números y caracteres especiales.

Diapositiva 20: Elemento 3: Frase.

Frase: pronto, esto será el estándar. Puede hacer que las contraseñas sean más largas usando frases cortas. Ejemplo: "vacas ayudan a hacer queso".

Diapositiva 21: Contraseñas seguras y fáciles de recordar. – Actividad 2

NOTA AL INSTRUCTOR: Dirija a los asistentes a la Actividad 2a y 2b en las páginas 2 y 3 de la Hoja de actividades.

Infórmeles a los asistentes que el grupo discutirá lo que se les ocurra, por lo que no deben usar sus contraseñas reales. El ejercicio es para practicar el uso de los métodos que el grupo acaba de ver: frases y combinaciones. Cuando los asistentes hayan completado las actividades, facilite un debate sobre lo que se les ocurrió a las personas.

Diapositiva 22: Informe de la Actividad 2a.

NOTA AL INSTRUCTOR: Use la diapositiva para informar sobre la actividad o como guía para usted mismo si está haciendo una demostración.

Diapositiva 23: Informe de la Actividad 2b.

NOTA AL INSTRUCTOR: Use la diapositiva para informar sobre la actividad o como guía para usted mismo si está haciendo una demostración.

Utilice la información del curso sobre las contraseñas seguras para analizar las respuestas de los participantes. Ejemplos que puede usar si necesita proporcionarlos:

1. *happybirthday - H@PPyBirthD@y0*
2. *josephsmith – 212Joe!Smith212*

Criterios: Las contraseñas deben tener cuando menos 12 caracteres y contener al menos una letra mayúscula, una letra minúscula, un número, y un carácter especial.

3. *1234567890 – unadoshebillasenmizapato*
4. *contraseña1 – mantenermicontraseñasegura*

Criterios: Las contraseñas deben tener al menos 12 caracteres sin ningún otro requisito de caracteres. Para hacer de esta una contraseña segura, use una frase corta.

Recordatorio: Las contraseñas más largas son contraseñas más seguras.

Diapositiva 24: Fraudes y estafas en línea.

Continuemos nuestro debate sobre la seguridad en línea con un vistazo a los fraudes y las estafas en línea. Cuando comenzamos el taller de hoy, hablamos de que la ciberseguridad tiene que ver con la seguridad de la información (nuestra identidad, nuestros datos personales y nuestros activos financieros) cuando estamos en línea.

Como dijimos, la ciberseguridad significa que 1) sus datos personales son accesibles solo para usted u otras personas que usted autorice, y 2) sus dispositivos (computadoras portátiles, computadoras de escritorio, teléfonos móviles, tabletas) funcionan correctamente y no tienen malware.

NOTA AL INSTRUCTOR: En caso de que se necesite una definición de malware: El malware es un software malicioso que puede tomar muchas formas: desde virus que infectan sus dispositivos favoritos hasta spyware y adware que rastrean sus actividades en línea.

Si bien podemos hacer todo lo posible para mantenernos seguros mediante el uso de sitios web seguros y contraseñas seguras para nuestras cuentas, también debemos estar al tanto de las diversas estafas en línea, en las que las personas intentan robar nuestra información. Pasemos a hablar sobre las diferentes formas en que las personas con malas intenciones intentan obtener acceso a su información personal y cuentas financieras. En otra palabras, los fraudes y las estafas en línea. Veremos cómo reconocer una estafa y cómo protegerse cuando vea una estafa.

Diapositiva 25: Fraudes y estafas en línea.

Algunos de los tipos más comunes incluyen el phishing (suplantación de identidad) y la ingeniería social. Estos tipos de estafas se pueden encontrar en un sitio web, en un correo electrónico o mensaje de texto, o incluso en una ventana emergente en su computadora.

Diapositiva 26: Phishing (suplantación de identidad).

Comencemos hablando del phishing, que es un tipo común de estafa. El phishing es cuando los estafadores usan correos electrónicos o mensajes de texto falsos para "pescar" información.

Estos mensajes falsos pueden parecer reales, pero enlazan a sitios web falsos. El sitio web puede parecer el de una compañía, organización o agencia gubernamental confiable y bien conocida, pero todo es un engaño para obtener información, como su número de Seguro Social o de su banco y los números de cuenta de sus tarjetas de crédito.

Diapositiva 27: Phishing (suplantación de identidad).

Un correo electrónico falso también se puede usar para infectar su computadora con software malicioso, que se conoce como malware, o con un virus tan pronto como abra el correo electrónico. El malware es una herramienta utilizada por los estafadores que puede adoptar muchas formas diferentes. Por ejemplo, el malware puede conducir a virus que infectan su computadora o a spyware que rastrea sus actividades en línea.

Diapositiva 28: Ingeniería social.

La ingeniería social es otro tipo común de estafa. Este es un nuevo nombre para un viejo truco de los estafadores. En este tipo de estafa, un impostor intenta ganarse su confianza al hacerse pasar por otra persona para obtener su información personal.

Por ejemplo, la persona puede afirmar ser un amigo o familiar en problemas, pretender ser una empresa con un descuento u oferta estupenda, o aseverar que trabaja en nombre de una agencia gubernamental, una organización o agencia de cobranza. Estos estafadores pueden ponerse en contacto con usted por teléfono, correo electrónico, mensaje de texto o a través de las redes sociales.

Diapositiva 29: Fraudes y estafas en línea.

NOTA AL INSTRUCTOR: Facilite un breve debate con los asistentes.

- ¿Cuáles son algunos ejemplos de phishing e ingeniería social que ha experimentado?
- ¿Cómo puede mantenerse a salvo de los estafadores?

NOTA AL INSTRUCTOR: Pida algunos ejemplos y, luego, pase a la siguiente diapositiva.

Diapositiva 30: Consejos para reconocer estafas.

Estas son algunas cosas en las que debe pensar cuando revisa correos electrónicos fraudulentos y otros intentos de phishing.

Las veremos una por una, y esta lista también se encuentra en su Folleto del alumno.

- ¿Ha escuchado hablar antes de la persona u organización?
- ¿Sabe de quién es el mensaje de correo electrónico?
- ¿Tiene errores el correo electrónico?
- ¿Le están solicitando su información?
- ¿Están intentando apresurarlo a tomar una acción rápida?
- ¿Es demasiado bueno para ser verdad?

Diapositiva 31: ¿Ha oído hablar de la persona u organización?

NOTA Al INSTRUCTOR: Comience haciendo la pregunta que figura en la diapositiva a los asistentes: ***¿Ha oído hablar de la persona u organización?***

Si es una empresa legítima, su logotipo oficial, dirección e información de contacto deben aparecer en su sitio web. ¿Ha oído hablar de esta empresa? ¿Está el logotipo de la empresa? ¿Hay información de contacto?

Este es un buen ejemplo de un sitio web comercial legítimo.

Diapositiva 32: ¿Sabe de quién es el mensaje de correo electrónico?

NOTA AL INSTRUCTOR: Comience haciendo la pregunta que figura en la diapositiva a los asistentes: ***¿Sabe de quién es el mensaje de correo electrónico?***

Este ejemplo afirma ser de PayPal. ¿Cuál es la dirección de correo electrónico del remitente? ¿Coincide?

La dirección de correo electrónico no coincide y no parece ser de PayPal. Esta es una clara señal de que es una estafa de phishing.

Diapositiva 33: ¿Le están solicitando su información?

NOTA AL INSTRUCTOR: Comience haciendo la pregunta que figura en la diapositiva a los asistentes: ***¿Le están solicitando su información?***

¿Están pidiendo información de su tarjeta de crédito u otra información personal? Los estafadores pueden afirmar que necesitan verificar o actualizar su información. Algunos estafadores también le pedirán que les hagan un giro de dinero o les envíen un depósito, prometiendo pagarle más a cambio.

En este ejemplo . . .

- el correo electrónico solicita al destinatario que confirme su identidad.
- el correo electrónico le pide al destinatario que inicie sesión usando el botón para proporcionar documentación.

Diapositiva 34: ¿Tiene errores el correo electrónico?

NOTA Al INSTRUCTOR: Comience haciendo la pregunta que figura en la diapositiva a los asistentes: ***¿El correo electrónico parece profesional o tiene muchos errores?***

¿Puede identificar errores en este correo electrónico? En este ejemplo, . . .

- la palabra "account" (cuenta) está mal escrita de diferentes maneras a lo largo del correo electrónico.
- la palabra “suspicious” (sospechoso) está mal escrita.
- hay un error gramatical: “please confirming provide the documents” (por favor, confirmar proporcionar los documentos).
- hay un espacio adicional entre “asked” (solicitó) y "to" (que) en el primer párrafo.

Si el correo electrónico es de una empresa legítima, no tendría esos errores.

Diapositiva 35: ¿Están intentando apresurarlo a tomar una acción rápida?

NOTA Al INSTRUCTOR: Comience haciendo la pregunta que figura en la diapositiva a los asistentes: ***¿Están intentando apresurarlo a realizar una acción rápida antes de tomarse el tiempo para pensarlo?***

¿Qué "frases o palabras alarmantes" está utilizando el estafador para dar urgencia a la solicitud?

En este ejemplo:

- el correo electrónico crea urgencia al sugerir que han estado tratando de comunicarse con usted.
- el mensaje incluye: “expiring soon” (que caduca pronto) en relación con la tarjeta de regalo.

Algunos estafadores intentan asustarlo para que actúe con rapidez. Lo amenazan con que sucederá algo malo, como que cerrarán una cuenta. Otros estafadores le prometerán algo bueno, pero solo si usted responde de inmediato.

Diapositiva 36: ¿Es demasiado bueno para ser verdad?

NOTA Al INSTRUCTOR: Comience haciendo la pregunta que figura en la diapositiva a los asistentes: ***¿Es demasiado bueno para que sea verdad, como que ganó el premio de un concurso en el que no recuerda haber participado?***

¿Qué suena "demasiado bueno para ser verdad" en este ejemplo?

En este ejemplo, al destinatario se le ofrece una tarjeta de regalo de $750.

Si suena demasiado bueno para ser verdad, probablemente lo sea.

Diapositiva 37: Actividad 3—Fraudes y estafas en línea

NOTA AL INSTRUCTOR: Dirija a los asistentes a la Actividad 3 en la Hoja de actividades. Cuando los asistentes hayan completado las actividades, realice un debate sobre lo que se les ocurrió a las personas.

Diapositiva 38: Informe de la actividad.

NOTA AL INSTRUCTOR: Use la diapositiva para informar sobre la actividad o como guía para usted mismo si está haciendo una demostración.

Las cosas que indican una estafa son . . . *(Señale cada respuesta en la diapositiva para repasarla con los alumnos).*

- el correo electrónico del remitente no es el de la farmacia. Además, incluye una cantidad excesiva de letras y números, a diferencia de la mayoría de las direcciones de correo electrónico comerciales.
- el correo electrónico incluye espacios adicionales entre palabras en las líneas 1, 3 y 4.
- el correo electrónico tiene errores gramaticales: “accounts coming in from palpability of account so the Pharmacy suspends the account service…” (cuentas procedentes de cuentas en evidencias por lo que la Farmacia suspende el servicio de cuenta) . . .”
- el correo electrónico incluye un archivo adjunto.

Diapositiva 39: Lo que se debe hacer y no hacer para evitar las estafas.

Aquí hay algunos consejos para mantenerse a salvo cuando se trata de estafas en línea. Los veremos uno por uno, y esta lista también se encuentra en su Folleto del alumno.

Diapositiva 40: No proporcione información personal.

No proporcione información personal a algo que podría ser una estafa. Esto incluye el nombre, la dirección de correo electrónico, el número de tarjeta de crédito o la contraseña.

Diapositiva 41: No responda ni se comunique con el impostor.

No responda ni se comunique con el estafador. Esto puede notificarle al estafador que se ha comunicado con una persona real, lo que puede dar lugar a más correos electrónicos fraudulentos.

Diapositiva 42: No haga clic en ninguno de los enlaces o botones.

No haga clic en ninguno de los enlaces o botones en un mensaje de correo electrónico de estafa. Esto puede llevarlo a sitios web no confiables.

Diapositiva 43: No descargue ningún archivo ni documento adjunto.

No descargue ningún archivo ni documento adjunto de un sitio web poco confiable. Pueden contener virus o malware que dañan su computadora o que recolectan su información personal.

Diapositiva 44: Sea escéptico.

Sea escéptico. Si cree que algo es una estafa, probablemente lo es.

Diapositiva 45: Lea los correos electrónicos con atención.

Recuerde leer atentamente los correos electrónicos y los mensajes de texto, asegurándose de que conoce al remitente. Aplique los otros consejos que presentamos para determinar si algo es una estafa.

Diapositiva 46: Busque la información de contacto por su cuenta.

Busque por sí mismo la información de contacto, los detalles sobre una empresa o la información de su cuenta. Vaya directamente al sitio web de la empresa o a la información de su propia cuenta para verificar. No visite ningún sitio web a través del correo electrónico fraudulento que le enviaron.

Diapositiva 47: Actividad 4.

En esta última actividad, practicaremos lo que hemos cubierto y veremos lo que todos han aprendido.

NOTA AL INSTRUCTOR: Recorra las siguientes diapositivas y anime a los alumnos a responder en grupo.

NOTA AL INSTRUCTOR: No es necesario hacer referencia a la Hoja de actividades del alumno para esta actividad.

Diapositiva 48: ¿Cómo sabe que un sitio web es seguro?

Respuesta: La dirección del sitio web comienza con HTTPS y se muestra un ícono de candado.

Los sitios que comienzan con "HTTPS" y un candado son sitios web que son seguros y protegen la información de su contraseña.

Diapositiva 49: ¿Cuál de estas contraseñas es la más segura?

Respuesta: vacasayudanahacerqueso

Las contraseñas más largas son más seguras. Es importante que no utilice información personal ni nada demasiado fácil de adivinar como contraseña.

Diapositiva 50: ¿Cuál es la mejor opción para recordar su contraseña?

Respuesta: Cuaderno guardado en un lugar seguro.

La opción más segura de estas tres es escribir la contraseña en un cuaderno que se guarda en un lugar seguro y protegido. Las demás personas pueden ver fácilmente una nota adhesiva en su computadora. Si usa su nombre y apellido, será fácil de adivinar para alguien que quiere acceder a sus cuentas.

Diapositiva 51: ¿Cuáles son tres cosas que indican que se trata de una estafa?

Respuestas:

- No sabe de quién es el correo electrónico.
- Nunca se ha registrado para obtener puntos en la farmacia.
- El mensaje tiene errores gramaticales.
- El mensaje está tratando de apresurarlo para que realice una acción.
- El mensaje dice que perderá algo si no actúa.
- El mensaje incluye un enlace que puede llevarlo a un sitio web nefasto o puede llevarlo a descargar un software malicioso.

Diapositiva 52: ¿Cuáles son tres cosas que indican que se trata de una estafa?

Respuestas:

- El mensaje no incluye su nombre, solo dice "Miembro adorable".
- “Miembro adorable” no es lo que podríamos llamar “profesional” para este tipo de correspondencia.
- Nunca se registró para el soporte técnico.
- El mensaje tiene errores gramaticales.
- El mensaje dice que ha gastado dinero que no gastó y está tratando de que reaccione.

Diapositiva 53: Recibe un correo electrónico que dice que ha ganado un premio. Usted piensa que es una estafa. ¿Qué debería hacer?

Respuesta: Colocarlo en su carpeta de correos no deseados o ignorarlo

Comunicarse con el remitente puede ocasionar que reciba más mensajes de correo electrónico no deseados. Hacer clic en cualquier enlace de un correo electrónico fraudulento puede ocasionar que reciba más mensajes no deseados y que lo lleve a sitios web inseguros.

Diapositiva 54: Preguntas

NOTA AL INSTRUCTOR: Averigüe si hay otras preguntas finales y responda las que hayan quedado pendientes en las secciones del "lugar de estacionamiento".

Diapositiva 55: Felicitaciones

En el día de hoy, usted . . .

- aprendió acerca de la ciberseguridad.
- desarrolló habilidades para
    - reconocer un sitio web seguro.
    - crear contraseñas seguras y fáciles de recordar.
    - reconocer y evitar las estafas en línea.
- aprendió consejos útiles para ayudarle a mantenerse seguro en línea.

*NOTA AL INSTRUCTOR: Proporcione a los asistentes un certificado de finalización***.**

Diapositiva 56: Capacitación adicional en línea.

NOTA AL INSTRUCTOR: Dirija a los alumnos a cursos adicionales que están disponibles. Dirija la atención de los alumnos a la dirección del sitio web que aparece en la diapositiva.

Diapositiva 57: ¡Gracias!

NOTA AL INSTRUCTOR: Finalice la sesión siguiendo estos pasos:

- *(Si corresponde): Mencione los talleres futuros de aprendizaje digital de AT&T y PLA planificados para el lugar y/o la comunidad.*
- *Averigüe si hay otras preguntas finales y responda las que hayan quedado pendientes en las secciones del "lugar de estacionamiento".*
- *"Gracias nuevamente a AT&T y a PLA por este taller. ¡Agradecemos a todos nuestros participantes por venir y les animamos a que sigan aprendiendo!"*