Orleans Digital Literacy Initiative

Seguridad en línea

Este módulo proporciona un vistazo general a la seguridad en línea. Cubre la creación de contraseñas seguras, el uso de un administrador de contraseñas, el uso compartido de cuentas, el phishing y cómo identificar estafas en línea.

Términos de ciberseguridad

→ La ciberseguridad es la práctica de mantener nuestras vidas digitales y nuestras computadoras seguras y protegidas.

Malware – Software malicioso destinado a dañar un sistema informático, ya sea para tomar información, exigir rescate, desactivar o algo más.

Virus - Un tipo específico de malware de computadora que se autorreplica y se propaga a otras computadoras.

Red - El conjunto de dispositivos informáticos conectados entre sí y generalmente relacionados con un hogar o negocio.

Internet - El conjunto más amplio de computadoras conectadas a través de numerosas redes interconectadas.

Antivirus - Software que escanea un dispositivo o una red para detectar y alertar sobre amenazas a la seguridad y neutralizar el código malicioso.

Autenticador - Un método a través del cual un usuario prueba su identidad a un sistema. Puede ser una contraseña, una huella digital, un escaneo facial.

Red Privada Virtual (RPV) - Tecnología que extiende una red privada y todo su cifrado, seguridad y funcionalidad en una red pública. Con ella, los usuarios pueden enviar y recibir mensajes como si estuvieran conectados a una red privada.

Datos en línea

Cuando Ud. publica o da información o datos en línea, es importante ser consciente de lo que está compartiendo y la posibilidad de mal uso.

Ud. siempre debe tener en cuenta la información y los datos cuando Ud. publique en plataformas de redes sociales, compre en línea, registre cuentas y cada vez que ingrese su información personal de identificación en un dispositivo.

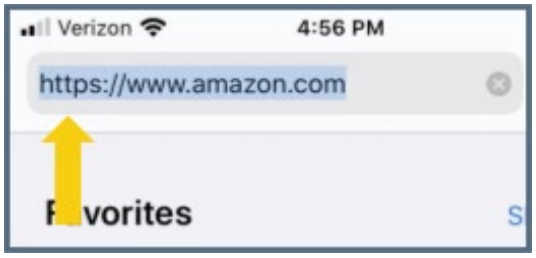
La **información personal de identificación** es cualquier información que se puede usar para descubrir quién es Ud. y potencialmente robar su identidad. Esto incluye su nombre, cumpleaños, dirección, número de Seguridad Social, información de tarjeta de crédito y más.

- ★ Asegúrese de que los archivos con información personal de identificación se almacenen en lugares donde su empleador u organización desee que se almacenen.
- ★ Asegúrese de que los archivos descargados a su computadora se borren para evitar que las personas que no deberían acceder a ellos los abran.
- ★ Asegúrese de que cualquier archivo o imagen que Ud. almacene en un dispositivo móvil se guarde en el lugar correcto y se elimine de cualquier lugar que no sea seguro, en caso de pérdida o robo del dispositivo.

HTTP versus HTTPS

¿Es seguro este sitio web?

Hay dos protocolos sobre cómo llega la información de su navegador a un sitio web y cómo llega del sitio web la información a su navegador. **HTTP** significa Protocolo de Transferencia de Hipertexto y **HTTPS** significa Protocolo de Transferencia de Hipertexto Seguro.



Amazon.com está usando HTTPS

La principal diferencia es que HTTPS es seguro (encriptado) y HTTP no lo es.

- ★ Alguien que intercepte maliciosamente nuestros datos cuando usamos HTTP puede ver o leer lo que hemos enviado
- ★ Alguien que intercepta maliciosamente nuestros datos cuando usamos HTTPS no puede ver o leer lo que hemos enviado

http *=protocolo*
www.mysite.com *=nombre del dominio*
/index.html *=recurso*

La estructura de URL de un sitio web alojado por http:

Nunca debe enviar información de identificación personal por HTTP. Solo envíelo por HTTPS. Nunca publique información de identificación personal en una unidad compartida como Google Drive o en un espacio de

calendario compartido. La información de identificación personal debe compartirse solo con aquellos que necesitan conocerla.

Algunas formas de verificar si un sitio web es legítimo pueden ser:

- ★ ¿Quién es el autor del recurso?
- ★ ¿Dónde se publicó el recurso?
- ★ ¿Qué información incluye el recurso?
- ★ ¿Por qué el autor creó el recurso?

Estafas & Phishing

¿Qué es una estafa?

Una estafa es un término que se usa para describir cualquier esquema fraudulento que toma dinero u otros bienes de una persona desprevenida. Las estafas en línea se han vuelto muy frecuentes. Aunque solían ser bastante obvios, se han vuelto más sofisticados en los últimos años. Las estafas pueden ser simples o más complejas. Son de naturaleza similar a las estafas telefónicas. Se pueden encontrar en correos electrónicos, sitios web y redes sociales. Recuerde: si algo parece demasiado bueno para ser verdad, ¡probablemente lo sea!

Tipos de Estafas

Una **Estafa de Donación** es cuando un estafador finge ser una organización benéfica para que usted le <<done.>> Sin embargo, en realidad termina dándole su dinero al estafador.

Catfishing es cuando un estafador crea una personalidad o identidad falsa para engañar a alguien para que le dé algo que quiere.

Una **estafa 419 o "Carta Nigeriana"** es una estafa en la que el estafador solicita que se le envíe una cantidad de dinero para cubrir algún costo para otorgar al destinatario de la carta/correo electrónico una gran suma de dinero.

Una **Estafa de Encuesta en Línea** es una estafa en la que un estafador generalmente ofrece dinero o un buen premio, como un iPad, pero usted debe completar una encuesta. Estas encuestas a menudo solicitarán información personal, especialmente la que se encuentra en las preguntas de seguridad, para tratar de identificarlo y obtener acceso a sus cuentas.

Los estafadores usarán correos electrónicos o mensajes de texto para engañarte y que les de su información personal. Pueden intentar robar sus contraseñas, números de cuenta o números de Seguro Social. Si obtienen esa información, podrían obtener acceso a su correo electrónico, banco, tarjetas de crédito u otras cuentas. Los correos electrónicos y mensajes de texto de phishing a menudo cuentan una historia para engañarlo para que haga clic en un enlace o abra un archivo adjunto.

Tácticas usadas en Estafas de Phishing:

- ★ Los estafadores dicen que han notado alguna actividad sospechosa o intentos del login
- ★ Pedirle que confirme su información personal
- ★ Pedirle que haga clic en un enlace para hacer un pago
- ★ Ofrezca un cupón para cosas gratis

Seguridad de contraseñas

Contraseñas seguras son efectivas para mantener su seguridad en línea.

Con una contraseña, se debe:

Crear una contraseña única para cada cuenta que usa.

Usar una mezcla aleatoria de números, letras, y símbolos.

Utilizar un procesador de contraseñas para gestionar sus contraseñas únicas.

Introducir las contraseñas solo en los sitios apropiados.

Con una contraseña, no se debe:

Usar frases comunes o información personal (por ejemplo, un nombre de una mascota)

Escribir sus contraseñas.

Compartir sus contraseñas.

Escoger contraseñas cortas.

Escoger una contraseña que se adivina fácilmente.

Usar la misma contraseña por mucho tiempo.

Guardar su contraseña en un lugar que se encuentra fácilmente.

Orleans Digital Literacy Initiative

Ejemplos de contraseñas buenas y malas

Ejemplos de contraseñas malas	Ejemplos de contraseñas buenas
Contraseña	@H76cxgV90$$jKTsk
Juan2021	IegtDL2021!
03-21-1990	S0pAd3VeRdURa5
Mago22	nwso^d-scr23ap(hk3dh

Guardar contraseñas fácilmente con procesadores de contraseñas

Una procesador de contraseñas guarda seguramente sus contraseñas y nombres de usuario, y también otra información que necesita estar privado, pero accesible. Algunas procesadores populares son LastPass, 1Password, o Dashlane. Procesadores tienen aplicaciones que usted puede descargar en su computadora o móvil y aplicaciones del Internet que usted puede acceder desde cualquier dispositivo. También tienen una variedad de planes gratuitas o de pago que serían apropiados para usted.

Lo mejor es evitar compartir información de cuenta cuando esto es posible. Sin embargo, algunas veces es imposible evitar compartir esta información con su familia. En esta situación, procesadores de contraseñas pueden ser útiles. Algunas le permiten registrar varios usuarios en una cuenta familiar o de negocios, algo que facilita la segura partición de contraseñas con alguien confiable. Otras le permiten invitar a un visitante a acceder solamente las contraseñas que quiere compartir. De cualquier manera, asegúrese de que confíe en esta persona y que no haya otra manera de compartir la misma información.

LastPass

1Password

Dashlan

La autenticación multifactor

La autenticación multifactor es cuando varios factores se necesitan para verificar la identidad. Después de entrar una contraseña correctamente, el sistema le enviará un código por mensaje de texto o le pedirá que obtenga un código de su aplicación de autenticación. Luego, necesitará entrar este código para finalizar el acceso.

La autenticación multifactor, también conocido como autenticación de dos factores, proviene un nivel extra de protección. La autenticación multifactor puede aumentar la seguridad en combinación con métodos de menor calidad (por ejemplo, una contraseña sencilla) porque individuos con malas intenciones no solamente tendrían que conocer su contraseña, sino también necesitarían acceso a su aparato para recibir el código desde una aplicación o mensaje de texto. La autenticación multifactor es ideal cuando la seguridad es más importante que acceso fácil. Note: Cuando tiene las opciones de una contraseña o biometría, biometría es siempre más fuerte que una contraseña complicada.

Ejemplos de biometría en un aparato son los escáneres de huellas dactilares o reconocimiento de cara.

Orleans Digital Literacy Initiative

Antivirus

Software antimalware es también conocido como software de antivirus. Es un tipo de software que ayuda a prevenir los virus en una computadora. Software antimalware puede escanear su computadora o escanear sus descargas para encontrar los virus. Es importante tener en mente que el software antimalware no previene todo tipo de virus, así que es importante usar otros métodos seguros.

Windows Defender es un buen antivirus software que viene pre-instalado en computadoras de Windows.

El logo de Windows Defender

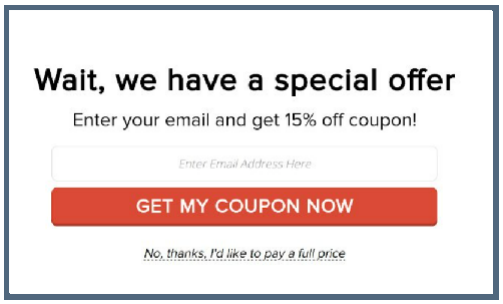
Como Protegerse Contra los Virus

Una de las mejores y mas fáciles cosas que puede hacer es mantener sus aplicaciones de software actualizadas con las versiones mas recientes que han sido proveídas por los creadores del software. Puede hacer que sus aplicaciones se actualicen solas y de ese modo recibir las versiones mas nuevas automáticamente. Otra acción que puede tomar es no visitar paginas, aplicaciones, o herramientas que no son confiables. Siempre asegúrese de no desactivar las configuraciones de antivirus. Finalmente, use el software de antivirus para escanear su computadora regularmente.

Ventana Emergente y Anuncios

Cuando usa un navegador de internet, tiene que tener en cuenta las ventanas emergentes y los anuncios.

Ventanas Emergentes son ventanas (o texto/cuadrados gráficos) que bloquean su acceso a una pagina o algo mas hasta que las cierra.
Anuncios son cosas que tratan de que hagas algo como dar clic e ir a paginas de compras. Ellos pueden ser maliciosos porque pueden obligarte a dar clic a algo, obtener información de usted, o intentar estafarlo.



Ejemplo de un anuncio de forma de ventana emergente

Es importante tener en cuenta que no todas las ventanas emergentes y anuncios son maliciosos. La manera de saber si una ventana emergente o anuncio es malicioso es analizar su contenido. Por ejemplo, si una pagina te pregunta por tu correo electrónico para un boletín informativo puede que no sea malicioso. Por otra mano, si una ventana emergente dice "¡Acaba de ganar un iPad gratuito!" o "Su computadora tiene 20 virus, ¡Límpiela ahora!" pueden ser maliciosos. Cosas importantes de tener en cuenta siempre son: ¿Es un contenido que tiene sentido con el de la pagina? ¿Es demasiado llamativo o demasiado bueno para ser verdad? **¿Esto es algo que debería darle clic?**

Seguridad para Redes Sociales

Consejo para Redes Sociales: ¿Hay una tendencia de redes sociales que crea un nombre de personaje divertido basado en cosas como su mes de nacimiento, segundo nombre, y la calle donde vive? Tenga cuidado con este tipo de publicación: ¡Su publicación pudiera ser usada para coleccionar información sobre usted!
Seria mejor no participar en esta tendencia.

Consejos para las redes sociales...

- ★ Sea cuidadoso y no comparta demasiado
- ★ Ajuste su configuración de privacidad
- ★ Verifique con quien se esta conectando
- ★ No comparta detalles personales
- ★ Recuerde que lo que pasa en el internet, se mantiene en el internet
- ★ Mantenga contraseñas fuertes

Orleans Digital Literacy Initiative

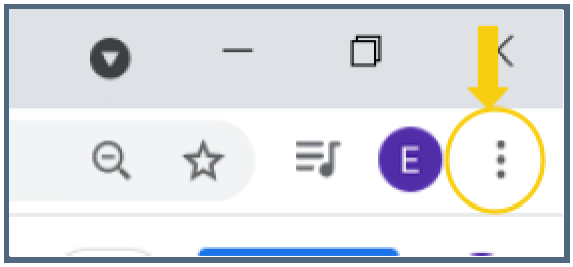
Descargando archivos

Al descargar archivos, estas son cosas importantes para recordar siempre

- ★ Asegúrese de confiar en el sitio web desde el que esta descargando.
- ★ Asegúrese de saber lo que está descargando
- ★ Asegúrese de hacer clic en el enlace correcto

Navegación de incógnito

Al navegar por Internet, hay ciertas cosas que se almacenan en su computadora, como **cookies**, que son piezas de información que se pueden usar para rastrear información de su navegación por Internet, y el **historial de navegación**, el cual es un registro de los sitios web que ha visitado. Si desea bloquearlos, puede utilizar la configuración de su navegador **incógnito**. Puede acceder al modo de incógnito de su navegador haciendo clic en el menú que generalmente se encuentra en la esquina superior derecha de su navegador y seleccionando "Nueva ventana de incógnito" o "Nueva ventana privada".



El primer paso para abrir un navegador en modo incógnito es hacer clic en los tres puntos en el lado derecho de su navegador.

El siguiente paso es elegir "Nueva ventana de incógnito", que abrirá una nueva ventana de incógnito.

El uso de una ventana de incógnito significa que no permanecerá conectado a ninguna de sus cuentas, no tendrá anuncios dirigidos ni la sesión aparecerá en el historial de su navegador. Esta es una buena manera de mantener sus sesiones de navegación más seguras en una computadora compartida.

Referencia de resumen de higiene digital

- ★ Asegúrese de que sus computadoras tengan el software actualizado
- ★ Utilice la autenticación de dos factores (2FA)
- ★ Tenga cuidado al hacer clic en enlaces o abrir archivos adjuntos en correos electrónicos
- ★ Implementar configuraciones de privacidad en cuentas de redes sociales
- ★ Instale software “anti-malware”
- ★ Usa contraseñas complejas
- ★ No utilice WiFi no seguro "gratuito"
- ★ Asegúrese de que los sitios web que visite utilicen HTTPS
- ★ No comparta sus dispositivos electrónicos
- ★ Deseche los dispositivos electrónicos de forma segura

Orleans Digital Literacy Initiative

Un consejo general de seguridad en línea.

Confié en tu instinto. Si un sitio web no le da una buena sensación, no envíe ninguna información confidencial.