Seguridad Informática

Guía Rápida

IES Diego de Praves

Riesgos de Seguridad

Las empresas de todo el mundo corren el riesgo de sufrir violaciones de seguridad. Aunque las empresas grandes y conocidas parecen ser un objetivo probable, las organizaciones pequeñas y medianas e individuos también están en riesgo. Hay muchas formas en las que los datos pueden verse comprometidos, incluyendo virus, fraudes de phishing, vulnerabilidades de hardware y software y agujeros de seguridad en la red.

¿Sabías qué?

11% de los adultos en Estados Unidos ha tenido datos personales robados

1 de 5 personas ha tenido una cuenta de correo o red social hackeada

98% de las aplicaciones de software son vulnerables

Solo el **40%** de los adultos sabe cómo protegerse en línea

Información Confidencial

Cuando se trata de seguridad, la confidencialidad, significa que la información privada nunca es vista por personas no autorizadas. La información confidencial solo debe ser accesible a las personas autorizadas para ver datos sensibles. Esta información incluye:

Información Personal

- Número de Seguridad Social
- Domicilio
- Historial salarial
- Problemas de desempeño
- Números de tarjetas de crédito

Información Empresarial

- Procesos
- Listas de clientes
- Investigación y desarrollo
- Estrategias de negocios
- Objetivos y proyecciones

Cortafuegos

Un cortafuegos actúa como un guardia de seguridad y previene que programas y personas no autorizadas intenten entrar en una red o computadora desde Internet. Existen cortafuegos basados en hardware que crean una barrera protectora entre redes internas y el mundo exterior, y de software, que comúnmente son parte del sistema operativo.

Contraseñas

Usar contraseñas que tengan al menos 8 caracteres e incluyan una combinación de números, letras mayúsculas y minúsculas, y caracteres especiales. Los hackers tienen herramientas que pueden descifrar contraseñas fáciles en solo unos minutos.

¿Cuánto tiempo toma descifrar una contraseña?

Existen 2 tipos de contraseñas:

Simples

Solo letras minúsculas

Complejas

Letras mayúsculas y minúsculas, números y caracteres especiales

Las contraseñas complejas son **EXPONENCIALMENTE** más difíciles de descifrar

¡Úsalas!

Este es el tiempo que toma descifrar una contraseña cuando es **simple** vs. **compleja**

Caracteres	Contraseña	Tiempo
8	ghiouhel	4 horas, 7 min
	ghiouH3l	6 meses
9	houtheouh	4 días, 11 horas
	Houtheo!2	1060 años
10	ghotuhilhg	112 días
	gh34uhilh!	1500 años
11	wopthiendhf	8 años, 3 meses
	w3pthi7ndh!	232,800 años
12	whithgildnzq	210 años
	@hi3hg5ldnq!!	15,368,300 años

Fuente: mywot.com

Malware

Malware se refiere a "software malicioso". Está diseñado para infectar la computadora que lo hospeda. Los tipos comunes incluyen:

VIRUS

Programa que se reproduce para infectar computadoras

ADWARE

Toma el control de la computadora o navegador y muestra molestos anuncios

SPYWARE

Rastrea en secreto las actividades e información en Internet

TROYANO

Programa malicioso que intenta engañar para ejecutarlo

Navegación en Línea

Los navegadores se comunican con los sitios web con un protocolo llamado HTTP que significa Protocolo de Transferencia de Hipertexto. HTTPS es la versión segura de HTTP. Los sitios web que usan HTTPS encriptan toda la comunicación entre el navegador y el sitio.

Los sitios seguros tienen un indicador, como un candado, en la barra de direcciones para mostrar que el sitio es seguro. Siempre se debe asegurar la seguridad al iniciar sesión o transferir información confidencial.

Los sitios sin HTTPS no son seguros y nunca deben usarse cuando se trata con datos personales. Si simplemente se está leyendo un artículo o revisando el clima, el HTTP es aceptable.

Seguridad de Red

- Usar seguridad de contraseña de Wi-Fi y cambiar la contraseña por defecto
- Establecer permisos para archivos compartidos
- Conectarse a una red de Wi-Fi pública, segura y conocida y asegurarse de que los sitios HTTPS habilitados se usan para datos confidenciales
- Mantener el sistema operativo actualizado
- Realizar revisiones de seguridad

Correo Electrónico y Phishing

Un correo electrónico de phishing trata de engañar a los consumidores para que proporcionen datos confidenciales para robar dinero o información. Estos correos electrónicos parecen ser de una fuente creíble, como un banco, entidad gubernamental o proveedor de servicio. Aquí hay algunas cosas para buscar en un correo electrónico de phishing:

Errores Gramaticales

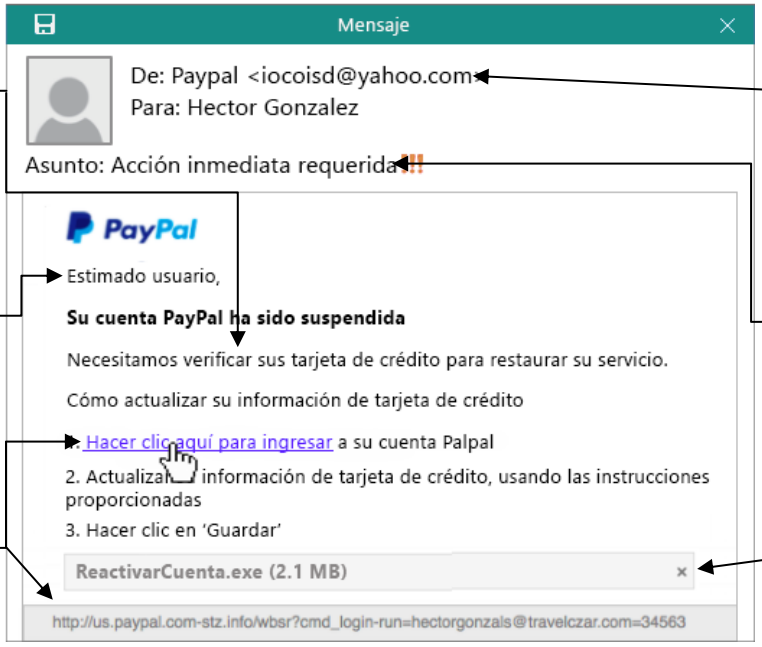
Errores de ortografía y mala gramática

Referencias Genéricas

No dirigirse por su nombre

Vista Previa

Siempre comprobar a dónde dirigen los vínculos antes de hacer clic



Dirección del Remitente

La dirección debe estar correlacionada con el destinatario

Acción Inmediata

Tener cuidado de cualquier cosa que requiera acción urgente

Archivos Adjuntos

Nunca abrir un archivo adjunto que no se está esperando