Conciencia sobre Ciberseguridad modulo 2 Cheat Sheet

by gonax133 via cheatography.com/211069/cs/45715/

Seguridad de Contraseñas

Siempre use una contraseña fuerte y única, y no reutilice contraseñas en diferentes sitios web.

Riesgos de Contraseñas Débiles y Reutilizadas

Riesgos financieros

Riesgos de privacidad

Riesgos de acceso a cuentas

Consejos para Contraseñas Fuertes

Evita la información personal	Avoid personal details in passwords (name, birthday, pet name).
Usa una mezcla de letras (mayúsculas y minúsculas), números y caracteres especiales.	Mezclar letras (mayúsculas y minúsculas), números y caracteres especiales fortalece las contraseñas.
Evita las palabras comunes del diccionario	Evita las palabras del diccionario; hacen que las contraseñas sean más fáciles de descifrar.
Usa un generador de contraseñas aleatorias	Usa un generador de contraseñas para obtener contraseñas fuertes y aleatorias.
No compartas tus contraseñas	Nunca compartas tus contraseñas con otras personas.
No anotes tus contraseñas	Nunca guardes tus contraseñas de forma insegura ni las escribas.
No envíes tus contraseñas por correo electrónico ni mensaje de texto	Nunca compartas tus contraseñas por correo electrónico, mensaje de texto o teléfono.

Sitios web no seguros

Sitios web con phishing, malware o software no deseado se consideran inseguros.

Medidas para evitar sitios web no seguros:

1)Busca "HTTPS" en la URL.

2)Evita los sitios proxy anónimos.

3)Verifica que haya un símbolo de candado en la barra de direcciones.

4)Usa navegadores modernos, que cuentan con filtros y herramientas de seguridad para bloquear sitios web inseguros.

Pop-up

Los anuncios emergentes(Pop-up) aparecen en nuevas ventanas mientras navegas y pueden ser intrusivos. Algunos anuncios emergentes instan a las personas a realizar una acción proporcionando información falsa, y pueden contener malware o enlaces maliciosos que podrían descargar ransomware o comprometer los sistemas.

Anuncio emergente malicioso

Requiere un pago	"¿Un anuncio emergente solicita un pago? Los sitios legítimos no usan ventanas emergentes para pagos."
Proporciona un número de teléfono para llamar	"¿La ventana emergente te pide que llames a un número? Verifícalo en el sitio oficial para evitar fraudes."
Incluye errores tipográficos, ortográficos y gramaticales	"Los errores tipográficos y gramaticales son señales comunes de fraude en línea."

Ventana emergente de scareware

"El scareware es una táctica de ingeniería social que utiliza ventanas emergentes para asustar a los usuarios y hacer que hagan clic en falsos eliminadores de virus o servicios de soporte técnico."

I. Engaña a los usuarios haciéndoles creer que su sistema está infectado.

II. Incluye un enlace de soporte falso o un número de teléfono.

III. Intenta extorsionar dinero o obtener acceso remoto.

IV. Muestra advertencias falsas de compromiso, a menudo con audio incesante.

V. Solicita instalar software de protección contra virus o eliminadores.

1. Mantente alerta.
2. Conoce las señales del scareware.
3. Contacta a tu equipo de ciberseguridad.

Amenazas cibernéticas en redes sociales

Las redes sociales conectan a personas y empresas, pero también conllevan riesgos de ciberseguridad.

Amenazas y vulnerabilidades a tener en cuenta:

Phishing

Ingeniería social

Malware

Robo de identidad

Secuestro de cuentas