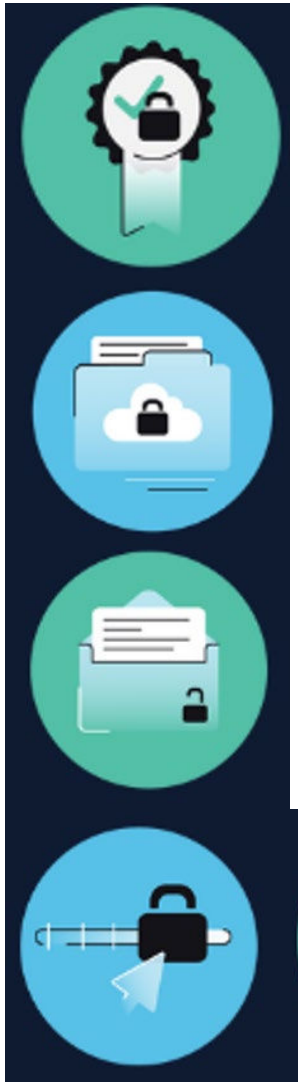
Concienciación sobre la Seguridad Cibernética



Piensa antes de hacer clic

No caigas en estafas de phishing. Reconoce y denuncia los correos electrónicos sospechosos.

Usa contraseñas fuertes

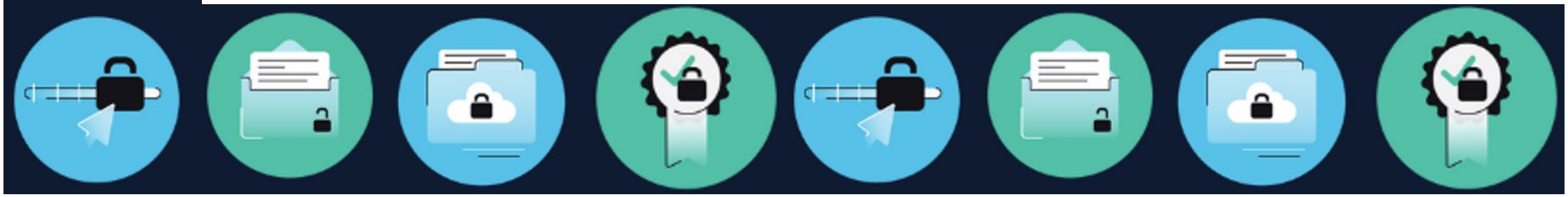
Utiliza contraseñas largas, únicas y generadas aleatoriamente. Utiliza administradores de contraseñas para almacenarlas.

Actualiza tu software

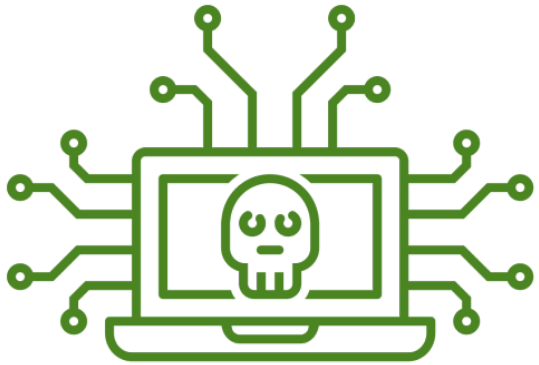
Actúe rápidamente para actualizar el software; mejor aún, activa las actualizaciones automáticas.

Habilita MFA

Exigir a los usuarios que habiliten MFA para iniciar sesión hace que sea mucho menos probable que sean hackeados.



Tipos de Ataque Cibernético



Malware

El 9% de los ataques cibernéticos que tuvieron lugar en los últimos 12 meses se debieron a infracciones de malware.

Denegación de servicios

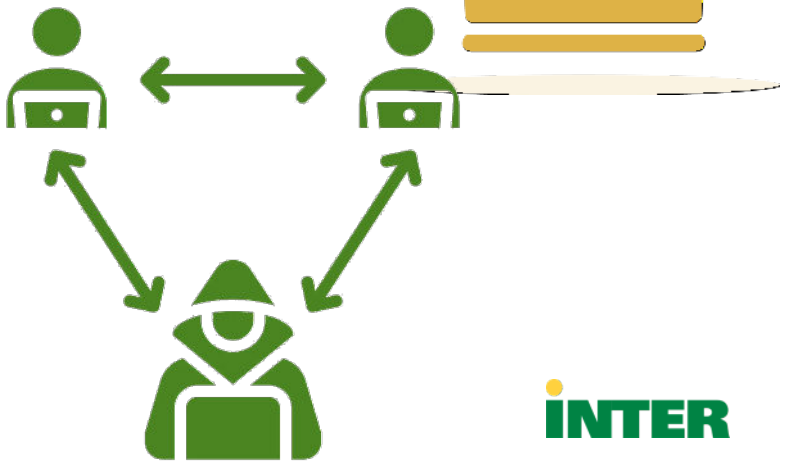
El 8% se debió a ataques de denegación de servicio (DOS).

Phishing

Los ataques de phishing son los más comunes con un 83% y han aumentado un 11% en los últimos 4 años.

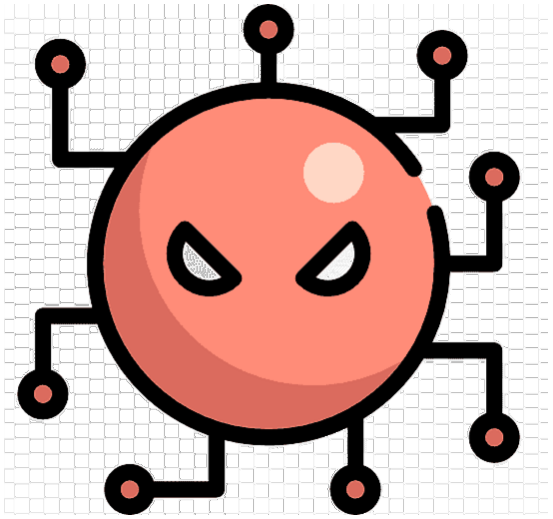
Ataque de intermediario

Menos del 5% de los ataques se debieron a ataques de intermediario



INTER

El **Phishing** es la práctica fraudulenta de enviar correos electrónicos que pretenden ser de empresas confiables con el fin de inducir a las personas a revelar información personal, como contraseñas y números de tarjetas de crédito. El **Malware** es un software diseñado específicamente para interrumpir, dañar o acceder de manera no autorizada a un sistema informático.



Disfrazar archivos adjuntos maliciosos como facturas falsas sigue siendo la táctica más popular para engañar a los usuarios y hacer que abran correos electrónicos de phishing y caigan en la trampa.

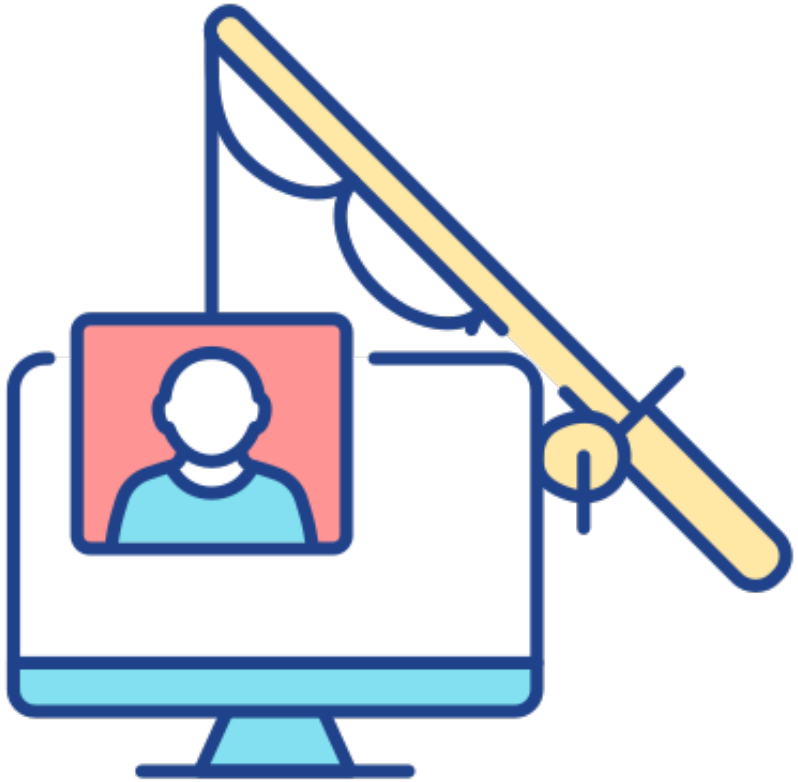
¿Cómo funciona el Phishing?

Recibes un correo electrónico o un mensaje de texto
Parece ser de alguien que conoces y te pide que hagas clic en un enlace o que proporciones tu contraseña, tu cuenta bancaria comercial u otra información confidencial.

Parece real
Es fácil falsificar logotipos e inventar direcciones de correo electrónico falsas. Los estafadores usan nombres de empresas conocidos o se hacen pasar por alguien que conoces.

Es urgente
El mensaje te presiona para que actúes ahora o algo malo sucederá.

¿Qué sucede después?
Si haces clic en un enlace, los estafadores pueden instalar ransomware u otros programas que pueden bloquear el acceso a tus datos y propagarse a toda la red de la empresa. Si compartes contraseñas, los estafadores ahora tienen acceso a todas esas cuentas.



¿Qué puedes hacer contra el Phishing?

Antes de hacer clic en un enlace o compartir información comercial confidencial:

Compruébelo

Busque el sitio web o el número de teléfono de la empresa o persona que se encuentra detrás del mensaje de texto o correo electrónico. Asegúrese de que se trata de la empresa real y no de descargar malware o hablar con un estafador.

Hable con alguien

Hablar con un colega puede ayudarlo a determinar si la solicitud es real o un intento de phishing.

Haga una llamada si no está seguro

Tome el teléfono y llame al proveedor, colega o cliente que envió el correo electrónico. Confirme que realmente necesitan información de usted. Use un número que sepa que es correcto, no el número que aparece en el correo electrónico o mensaje de texto.

Contraseñas: Qué se debe y no se debe hacer

- ✓ Utilizar la autenticación de dos factores.
- ✓ Utilizar varias palabras que no estén relacionadas.
- ✓ Utilizar una contraseña diferente para cada aplicación "elefanteazulvelagranja“.
- ✓ Utilizar un administrador de contraseñas.

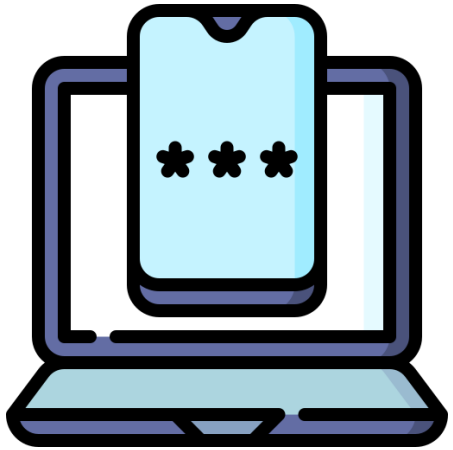
- × **NO** confiar sólo en las contraseñas.
- × **NO** contraseñas fáciles de adivinar o reutilizar.
- × **NO** crear contraseñas difíciles de recordar "&pck1s0mmz“.
- × **NO** anotar las contraseñas.

Protege tu información personal

Contraseñas seguras:

Usa contraseñas largas y complejas.

No reutilices contraseñas en diferentes sitios.



Autenticación de dos factores:

Añade una capa extra de seguridad a tus cuentas.

Cuidado con Phishing:

No abras correos electrónicos o enlaces sospechosos.

Estafas de Apoyo Técnico Falso

Recibe una llamada telefónica, una ventana emergente o un correo electrónico que le informa que hay un problema con su computadora.

A menudo, detrás de estas llamadas, mensajes emergentes y correos electrónicos se encuentran estafadores que quieren obtener su dinero, información personal o acceso a sus archivos. Esto puede dañar su red, poner en riesgo sus datos y perjudicar su negocio.

¿Qué hacer en caso de un incidente de seguridad?

Identificación:
Reconoce señales de que algo está mal (p. ej., actividad inusual en una cuenta).

Reporta:
Informa inmediatamente al equipo de Informatica de la universidad.

No entres en pánico:
Sigue los procedimientos establecidos para incidentes de seguridad.

Cómo Proteger Equipos y Archivos en Papel

Limite el acceso físico

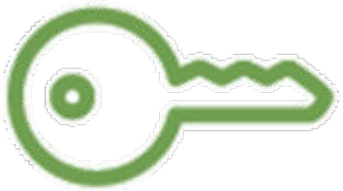
Cuando los registros o dispositivos contengan datos confidenciales, permita el acceso solo a quienes los necesiten.

Mantenga inventario

Identifique y proteja los dispositivos que recopilan información confidencial. Conserve solo los archivos y datos que necesita y sepa quién tiene acceso a ellos.

Almacenar de forma segura

Cuando los archivos en papel o los dispositivos electrónicos contengan información confidencial, guárdelos en un armario o habitación cerrados con llave.



Enviar recordatorios

Recuerde a los empleados que guarden los archivos en papel en archivadores cerrados con llave, cierren la sesión de su red y aplicaciones, y nunca dejen archivos o dispositivos con datos confidenciales sin supervisión.