



Phishing

QUE NO TE PESQUEN

Phishing es la estafa cometida a través de medios digitales (correo, redes sociales...) mediante la cual se intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta

Seguro te conectás

Consejos

- ✓ No compartas ni envíes tus usuarios y contraseñas, sin importar quién los pida.
- ✓ No accedas a páginas web a través de enlaces (links) en correos electrónicos enviados por desconocidos.
- ✓ Nunca respondas brindando tu información personal a quien no conocés. Si recibís un correo desconocido, no confíes solo por ver tu nombre en él.
- ✓ Eliminá los correos de remitentes desconocidos.
- ✓ Ingresá tu información personal solamente en páginas web seguras. Mirá la barra del navegador; si dice "https" y es la dirección web correcta, es segura.



Ransomware

QUE NO TE AGARREN DESPREVENIDO

El ransomware es el equivalente informático a un secuestro. Es un tipo de ataque que te restringe el acceso a la información de tu equipo. De esta manera, el atacante puede exigirte un pago a cambio de quitar esa restricción.

Seguro te conectás

Consejos

- ✓ Asegurate de que tus archivos de trabajo estén respaldados.
- ✓ Mantené actualizados tu sistema operativo y la versión de navegador que usás o solicitá asistencia al área de soporte informático de tu organización.
- ✓ No abras contenidos adjuntos sospechosos que te lleguen por correo electrónico o redes sociales.
- ✓ Eliminá sin abrir toda comunicación sospechosa, incluso si proviene de tus contactos.
- ✓ Si el antivirus te alerta de una amenaza, contactá al área de soporte informático de tu organización.
- ✓ No respaldes información en tu propia computadora o en un sitio accesible directamente desde ella. Si tu computadora se ve comprometida, tu respaldo también lo estará.



Contraseñas seguras

NO TE REGALES

La contraseña es la llave para proteger toda tu información digital y la del lugar en el que trabajás.

Seguro te conectás

Consejos

- ✓ Jamás compartas tus contraseñas, no importa quién te las pida.
- ✓ Usá contraseñas que tengan como mínimo 8 caracteres.
- ✓ No uses como contraseña: tu nombre personal o de usuario, documento, fecha de nacimiento o claves numéricas.
- ✓ Cuando elijas tu contraseña combiná Mayúsculas, minúsculas, c@racteres especiales y núm3r0s.
- ✓ Puedes usar una frase como contraseña, eso te permitirá recordarla más fácilmente.
- ✓ Cuando utilices contraseñas en un equipo que no es tuyo, no selecciones "Recordar contraseña".

Escritorios limpios



CUIDÁ TU INFORMACIÓN

Es posible que en tu lugar de trabajo tengas impresos y/o anotaciones con información confidencial que debés cuidar.

Seguro te conectás

Consejos

- ✓ Guardá documentos impresos y medios de almacenamiento con información confidencial en un lugar seguro.
- ✓ No dejes información sensible al alcance de cualquiera.
- ✓ Recordá bloquear el usuario (Win +L) antes de ausentarte de tu computadora.
- ✓ Retirá siempre los documentos que mandes a imprimir, principalmente cuando se trate de impresoras compartidas.
- ✓ Antes de retirarte, borra la información de pizarrones y carteleras.