Guía. Correos fraudulentos

Identifica los correos potencialmente peligrosos

- SOSPECHA SI no proviene de cuentas oficiales, aunque parezcan cuentas fiables de profesorado, alumnado, centros o personas conocidas. Si son correos de la Consejería de Educación comprueba siempre que el remitente es una **cuenta institucional.** Puedes comprobar las cuentas institucionales desde las que se pueden enviar correos en el Directorio Consejería de Educación: comprobar cuentas institucionales

- SOSPECHA SI tiene remitentes con direcciones de correo inusuales o poco creíbles: nombres propios; combinaciones de letras, dígitos, símbolos, incluso con nombres de marcas conocidas; dominios extraños; cuentas muy largas, etc.

- SOSPECHA SI contienen:
  - **Advertencias que generan sensación de urgencia:** *Abra documento disponible en…, Su cuenta se eliminará si no hace…, Se requieren sus datos para evitar…,* etc.
  - **Enlaces**: suelen llevar a ventanas en las que hay que introducir datos o credenciales. Sospecha de direcciones muy largas con puntos, guiones, con combinaciones de letras, dígitos y símbolos; dominios extraños; etc.
  - **Premios**, sorteos, herencias, pagos a cuenta para conseguir beneficios millonarios, ofertas imposibles. La mejor defensa es el sentido común.
  - **Imitación de la imagen corporativa de entornos conocidos** (Principado, Educastur, Microsoft, Google…). Cada vez es más frecuente la copia total o parcial de comunicaciones oficiales que reproducen fielmente su estilo, formato e imagen corporativa; por ello, un correo correctamente redactado y con apariencia legítima no garantiza que sea auténtico.
  - **Textos sospechosos.** Redactados en otros idiomas o en español con traducciones de mala calidad: tiempos verbales mal utilizados, ausencia o trastoque de preposiciones, palabras en desuso, sin tildes, etc. Si el correo tiene partes correctamente redactadas (probablemente copias) revisa siempre las partes añadidas por los *phishers*.

Cuando recibas un correo sospechoso…

- NUNCA pulses en ningún enlace ni abras o descargues archivos adjuntos. Como mínimo, su finalidad es robar datos y credenciales o introducir *malware* en el equipo. Phishing. Guía para identificar enlaces y adjuntos sospechosos (INCIBE)

- NUNCA facilites datos personales, claves, PIN de tarjetas… ni respondiendo por correo ni en ninguna web a la que hayas accedido desde estos correos. Ninguna entidad seria pedirá este tipo de datos por este medio.

- DENUNCIA el correo como *phishing*: botón derecho sobre el correo, opción *Denunciar/Informar sobre phishing.*

- ELIMINA el correo de tu bandeja de entrada y de la carpeta de elementos eliminados.

- CAMBIA TU CLAVE lo antes posible si ya has hecho clic en algún enlace, descargado un adjunto o introducido tus credenciales.
  Información: gestión de cuentas y claves

Recomendaciones generales

- CUIDA TUS CREDENCIALES. Nunca dejes a nadie tus credenciales; **no utilices la cuenta educativa para usos ajenos a educación, especialmente para registrarse en plataformas como redes sociales, juegos, comercio online, etc.** El riesgo es que puedan capturar tu cuenta y suplantarte, enviar *phishing* o mensajes a redes sociales en tu nombre; robar y difundir tus datos personales, tus fotos, etc.; realizar acciones de lucro económico a tu costa; promover el ciberacoso, etc.

- CONTRASEÑAS
  - **Usa contraseñas robustas:** mínimo 12 caracteres, con combinaciones de mayúsculas, minúsculas, números y caracteres especiales. Sin nombres, fechas o cadenas de caracteres fácilmente reconocibles.
  - **Cambia las contraseñas** a menudo, siempre que la aplicación lo requiera y siempre que sospeches que pueda haber algún ataque.
  - **Nunca marques *recordar contraseña*** (especialmente en equipos ajenos). Te ahorrarás escribir la contraseña, pero puedes perder mucho más.

- PROTEGE TUS DISPOSITIVOS con software antivirus, cortafuegos... Bloquea los dispositivos siempre que dejes de usarlos o que queden sin vigilancia. No uses nunca USB o unidades externas ajenas que pueden contener virus o *malware*.

- SESIÓN DE TRABAJO
  - **Nunca marques *mantener sesión iniciada*** (especialmente en equipos ajenos). Te ahorrarás iniciar sesión, pero puedes perder mucho más.
  - **Cierra tu sesión cuando termines de trabajar.** El aspa del navegador no cierra sesión; busca el *cierre de sesión* en cada aplicación (suele estar asociado a la ficha de perfil). Esto es especialmente importante en los equipos de uso colectivo en los centros educativos.
  - **Navegación privada:** en los dispositivos ajenos, borra los datos de navegación cuando termines o usa en tu navegador opciones de *navegación privada* o de *incógnito*.

- COMPETENCIA DIGITAL. Procura estar al día de las novedades tecnológicas y de los fraudes comunes. Contribuye a que el alumnado sea consciente de los riesgos del uso de herramientas en internet, de proteger sus identidades digitales y **del uso exclusivamente educativo de sus cuentas institucionales.**

- Toma precauciones en el mundo digital como las tomas en el mundo real.

Más información: Internet seguro y protección de datos (Educastur)