Consejos de seguridad en el uso de e-mails

El mero uso de correo electrónico supone afrontar unos riesgos que pueden ser evitables siguiendo unos sencillos consejos:

Contraseñas

- Cambie su **contraseña** con frecuencia.
- Utilice **contraseñas seguras**. Nunca use una contraseña que contenga "contraseña" o "12345678", ni incluya una fecha importante, etc.
- Utilice una **contraseña diferente** para cada una de sus cuentas. Si utiliza la misma contraseña para su cuenta de banco al igual que para su cuenta de correo electrónico, usted se convierte en un objetivo mucho más vulnerable frente al robo de datos.
- Cuando se dé de alta en otros servicios que le piden su dirección de correo y una contraseña, **nunca proporcione la contraseña que usa para la cuenta de e-mail**, pues no le está pidiendo dicha contraseña, sino que debe establecer otra específica para ese servicio.

Documentos adjuntos

- No abra un **archivo adjunto** a menos que sepa de quién es y que realmente espere ese archivo, pues al abrirlo puede instalarse malware (virus, programas que bloquean los ficheros, programas bots o zombie para lanzar ataques a terceros, etc)
- Utilice el **software anti-virus** en su máquina local, y asegurarse de que está actualizado con las últimas definiciones de virus.
- Si recibe un archivo adjunto de alguien que no conoce, **no lo abra**. Bórrelo inmediatamente.

Phishing y otros ataques de ingeniería social

El **Phishing** es uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. El estafador, *se vale de técnicas de ingeniería social,* haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico. Para evitar el phising:

- No haga caso a mensajes que soliciten información personal como contraseñas de cuentas bancarias, tarjetas de crédito o números de la Seguridad Social. Esa información sensible nunca debe ser suministrada como respuesta a un e-mail, aunque parezcan
- Los mensajes de phising contienen direcciones de correo electrónico sospechosas con dominios muy parecidos a los legítimos.
- Si sospecha de un correo de phising, informe a los Cuerpos y Fuerzas de Seguridad del Estado para que investiguen el posible delito tecnológico:
    - Guardia Civil (Grupo de Delitos Telemáticos):
      https://www.gdt.guardiacivil.es/webgdt/pinformar.php
    - Policía Nacional (Delitos Tecnológicos)
      https://www.policia.es/colabora.php

Enlaces a internet (URLs)

Los correos electrónicos recibidos de fuentes no confiables pueden redireccionarnos a webs potencialmente peligrosas. Se recomienda:

- **Pase el cursor** del ratón sobre los enlaces antes de hacer clic sobre ellos para ver si la URL indica la dirección adecuada.
- **No entre** en una web que sospeche pueda ser maliciosa.

Otros consejos

- **No dé su dirección** de correo electrónico a los sitios que no sean de confianza.
- **No publique** su dirección de correo electrónico de sitios web públicos o foros. A menudo los spammers escanean estos sitios para encontrar nuevas víctimas de correo.
- No haga clic en el enlace "**Darse de baja**" en un mensaje de spam. Sólo le haría saber al spammer que su dirección es legítima, lo que podría dar lugar a que recibir más spam.
- Comprenda que las empresas reconocidas **nunca le pedirán** información personal por correo electrónico.
- **No envíe información personal** en un mensaje de correo electrónico.
- **No responda** a correo no deseado.
- **No comparta** las contraseñas.
- Asegúrese de **cerrar la sesión**

Fuente: https://www.interbel.es