GUIAS DE SEGURIDAD UJA

Seguridad en el correo electrónico

1. Introducción

Según recientes estadísticas, en el mundo existen más de 500 millones de usuarios de correo electrónico, lo que supone un enorme mercado para organizaciones y personas con fines maliciosos.

No se trata de ser alarmistas, pero la realidad es que en Internet existen todo tipo de trampas y artimañas diseñadas para obtener algún tipo de beneficio de los usuarios, y actualmente la mayor parte de esas amenazas llegan en forma de mensajes de correo electrónico.

En esta guía pretendemos identificar cuales son esas amenazas y al mismo tiempo, ofrecer una completa lista de consejos y medidas a tener en cuenta para seguir haciendo uso de un sistema de comunicación tan habitual como es el correo electrónico, con las mayores garantías de seguridad.

2. Peligros más frecuentes asociados al correo electrónico

- **SPAM (correo basura)**: más del 80% de correos electrónicos enviados en todo el mundo actualmente son SPAM, y este porcentaje sigue creciendo.

- ***Phishing* (captura de credenciales)**: consiste en un método fraudulento de capturar información sensible, como nuestros números y claves de cuentas bancarias o de tarjetas de crédito. Se nos intenta engañar con mensajes que aparentan ser mensajes oficiales de entidades financieras o empresas de nuestra confianza.

- **Estafas de todo tipo**: donde se nos intenta vender productos falsos o inexistentes, se nos solicita dinero aludiendo a buenas causas, ofertas de trabajo inexistentes, y un largo etcétera.

- Correos con **ficheros adjuntos maliciosos (virus, gusanos, troyanos…)**. Muchos de estos ficheros infectados a menudo utilizan la libreta de direcciones de nuestro cliente de correo para renviarse a su vez a todos nuestros contactos.

- **Cadenas de mensajes falsos (hoaxes o bulos):** generalmente se trata de mensajes variados acerca de hechos o falsas alarmas de cualquier tipo, en los que se nos pide que reenviemos y difundamos el mensaje entre nuestros conocidos.

3. Consejos para un uso seguro del correo electrónico

3.1. Consejos de carácter general

- **Usar diferentes cuentas de correo electrónico:** Se recomienda usar dos o tres cuentas diferentes: una para el trabajo, otra para uso personal y una tercera para subscripciones y recepción de información.

- No usar de forma habitual el correo electrónico para enviar y recibir información sensible. Si necesita enviar datos importantes o sensibles a través de correo electrónico, asegúrese de que los protocolos de envío (SMTP) y recepción (POP3/IMAP) de correo configurados en el cliente son seguros. **En el caso de las cuentas de correo de la UJA, se recomienda la configuración de estos protocolos seguros (cifrados) de correo: SMTP Seguro (puerto 25 con TLS), POP3S (puerto 995 con SSL) e IMAPS (puerto 993 con SSL).** Puedes consultar las guías de configuración segura de correo en la siguiente dirección:

https://www.ujaen.es/servicios/sinformatica/guias-practicas/correo-electronico

- **Usar la opción de copia oculta (BCC):** Cuando incluimos las direcciones de correo electrónico de una persona en el campo "BCC" ninguno de los receptores puede ver las direcciones de los otros receptores de correo electrónico, mientras que, si utilizamos "CC", si se verán los destinatarios.

- **Ser prudente a la hora de contestar.** Aunque los clientes de correo suelen tener por defecto la opción de contestar sólo al remitente, a veces por error podemos seleccionar la opción de "Contestar a todos" e incluir a todos los que estaban en el correo electrónico original en la respuesta, con las consecuencias que ello pueda tener.

- En muchos casos, el SPAM proveniente del **reenvío de correo electrónico.** Sólo se necesitan unos pocos segundos para borrar todas las direcciones de mail recibidas antes de reenviar una parte o la totalidad del correo, y ello puede evitar que, por nuestra culpa, nuestros contactos sean víctimas de SPAM o phishing.

3.2. Para evitar el correo electrónico fraudulento:

- **Aprende a reconocer los fraudes por correo electrónico.** Ten especial cuidado en no abrir y elimina directamente aquellos correos en los que:

    - Nos informen de que hemos ganado en cualquier tipo de sorteo o que vamos a recibir cualquier tipo de premio.

- Correos en los que nos informan de reyes o príncipes de Nigeria tratando de enviarnos una enorme cantidad de dinero.
- Los detalles de ninguna cuenta bancaria en ningún caso necesitan ser reconfirmados inmediatamente.
- Si nos informan de algún tipo de herencia sin reclamar.
- Si nos indican que hemos ganado cualquier tipo de dispositivo electrónico o nos informan de alguna oferta sospechosa.
- Cualquier otro tipo de correo que nos resulte altamente sospechoso y que provenga de remitentes que no conocemos.

- **Aprende a reconocer los ataques de phishing en los mensajes de correo electrónico.** Aunque seamos el usuario de correo electrónico más experimentado del mundo, antes o después acabaremos abriendo algún correo electrónico de phishing. En este punto, la clave para limitar el daño está en reconocer este tipo de mensajes.

- Las pistas que nos pueden hacer sospechar de un phishing incluyen:

  - Un logotipo que parece distorsionado o de mala calidad.
  - Mensajes que se refieran a nosotros como "estimado cliente" o "estimado usuario" en lugar de incluir nuestro nombre real.
  - Mensajes que nos adviertan que una cuenta nuestra se cerrará a menos que confirmemos nuestra información inmediatamente.
  - Mensajes que vengan de una cuenta de correo similar, pero diferente a una que la compañía real que nos envía el correo usa normalmente.
  - Mensajes que informan de "amenazas a la seguridad" y requieren que actuemos inmediatamente.

- En estos casos, la mejor defensa es no abrir nunca dicho mensaje. Y en caso de abrirlo, nunca debemos contestar ni hacer clic en ningún enlace incluido en el mensaje.

- Nunca envíes información sensible por correo electrónico y nunca proporciones información sensible a través de ningún enlace ni formulario que aparezca en el correo electrónico que has recibido.

- **Nunca proporciones tus contraseñas a nadie. ¡Son totalmente personales! Si se las proporcionas a terceros, las acciones que realicen las harán en tu propio nombre.**

3.3. Para evitar el malware a través de correo electrónico:

- **Nunca abraa ningún mensaje ni fichero adjunto de un remitente que desconozcas o que te resulte sospechoso.** Elimina directamente este tipo de mensajes.

- Es importante mantener actualizado el **software antivirus** y tenerlo configurado para que analice todos los correos electrónicos entrantes.

- Habilitar en el cliente de correo los **filtros de correo electrónico no deseado**.

3.4. Otros consejos

- **No compartas la información de tu cuenta de correo con otros.**

- **No uses contraseñas simples y fáciles de adivinar.** Cuando

crees una contraseña usa números poco comunes y combinaciones de letras que no formen una palabra que se puedan encontrar en un diccionario. Una contraseña segura debe tener un mínimo de ocho caracteres, usando mayúsculas y minúsculas, números y caracteres especiales (%, &, $...).

- Como consejo adicional, cambia tus contraseñas (incluidas las del correo electrónico) de forma periódica, al menos una vez al año.

- **Cifra tus correos electrónicos importantes.** Para ello, debes disponer de un certificado digital.

4. Seguridad en el correo electrónico de la UJA

4.1. Sistema anti-SPAM centralizado

La Universidad de Jaén dispone de un sistema anti-SPAM para atenuar el aumento de las amenazas a la seguridad contenidas en el correo, tales como SPAM, phishing, virus, etc... Este sistema incorpora una serie de filtros que protegen el correo de la UJA (Filtro de reputación, filtro antivirus y filtro de contenidos).

4.2. Filtros de correo no deseado en GMail

Gmail incluye filtros de correo no deseado que ayudan a proteger nuestra cuenta de las amenazas más habituales (SPAM, *phishing*…). Podemos ir alimentando y entrenando estos filtros a partir de los correos que recibimos en nuestra bandeja de entrada de Gmail.

Cuantos más mensajes marquemos como spam, más eficaz será la clasificación automática de spam de Gmail. Para ello, simplemente tenemos que seleccionar uno o varios mensajes y hacer clic en **Marcar como spam**  .

Si en algún momento marcamos un correo incorrectamente, podemos quitarle la etiqueta de spam. Para ello, dentro de Gmail en el lateral izquierdo, haremos clic en **Más** y en la carpeta **Spam**. Abrimos el correo marcado incorrectamente y en la parte superior, haremos clic en **No es spam**.

Para impedir que un tipo de mensajes se coloque en Spam en el futuro, una de las formas de evitarlo es añadir el remitente a nuestros contactos.

5. Referencias en Internet

- Universidad de Jaén: Guías prácticas relacionadas con el correo electrónico
  https://www.ujaen.es/servicios/sinformatica/guias-practicas/correo-electronico
- Medidas de seguridad en el correo de Google
  http://support.google.com/accounts/bin/answer.py?hl=es&answer=46526
- Decálogo de seguridad para el correo electrónico
  http://www.baquia.com/blogs/seguridad/posts/2012-10-09-decalogo-de-seguridad-para-el-correo-electronico
- Instituto Nacional de Ciberseguridad (INCIBE)
  https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-correo-electronico.pdf
- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/
- CCN-CERT
  https://www.ccn-cert.cni.es/
- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es
- Policía Nacional – Brigada de Investigación Tecnológica
  https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html