

Tratamiento de la Información y Competencia Digital (TICD)

Acceso Ciclos Formativos de Grado Superior (ACFGS)

Tema 2. Seguridad y ética informática

Tema 2. Parte 2. Seguridad en internet

Resumen

Paco Aldarias. 22/10/2024



Índice

1. **Introducción**
2. Prácticas de seguridad recomendadas
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

1. INTRODUCCIÓN

*pirata informático puede ser:

Cracker = quiere hacer daño

Hacker = no quiere hacer daño

- Los virus informáticos son de Windows. No hay ni en Linux, ni Mac.
- Windows permite infectar fácilmente el sistema informático.
- Los primeros virus eran diseñados para destruir y colgar ordenadores.
- Actualmente, los creadores de software malicioso (malware) tienden a tener incentivos (motivos) económicos.
- Los piratas* pueden robar la información privada con propósitos económicos, o pueden controlar nuestros hábitos de navegación en Internet para proporcionarnos publicidad a medida.

1. INTRODUCCIÓN

```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19    3 JOBS
LOAD AV    3.87    2.95    2.14
JOB TTY  USER      SUBSYS
1  DET  SYSTEM     NETSER
2  DET  SYSTEM     TIPSER
3  12   RT         EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

EL virus creeper lo creo en 1971 Bob Thomas que se replicaba por la red ARPANET
Mostrando el mensaje cogeme si puedes.

Índice

1. Introducción
2. **Prácticas de seguridad recomendadas**
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

*Un agujero del SO es una vulnerabilidad no reparada (parcheada).

2. PRÁCTICAS DE SEGURIDAD

1. Utiliza un **antivirus que ANALICE** todo **lo QUE** descargas
 - a. Asegúrate de tener un antivirus instalado
 - b. Mantén tu antivirus actualizado
 - c. Realiza análisis regularmente de todo el sistema.
2. Mantén el sistema operativo (SO) y el navegador actualizado
 - a. Los virus aprovechan los **agujeros del SO*** y navegador para infectar tus dispositivos
 - b. **Los fabricantes corrigen las aplicaciones a través de actualizaciones (parches)**
 - c. Activa las actualizaciones automáticas de tu SO, navegador, plugins del navegador y resto de aplicaciones
3. Cuida tus contraseñas
 - a. Asegúrate de estar en la página correcta cuando las introduzcas
 - b. **No utilices la misma contraseña en diferentes servicios**
 - c. No compartas tus contraseñas con nadie
 - d. **Mays/mins, núms, caract. especiales y +8 caracteres**

2. PRÁCTICAS DE SEGURIDAD

4. Confía en la Web pero no seas ingenuo

- a. No todo lo que se dice en Internet es cierto. **Solución: Descarga software SIEMPRE desde su dominio oficial**
=> El dominio oficial debe aparecer en la barra de título o en la barra de estado
- b. **Si tienes dudas, contrasta la información con otras fuentes.**
Puedo usar Wikipedia? Sí! Pero contrastando su información

5. **No hagas clic en enlaces que resulten sospechosos***

- a. Sé precavido al seguir enlaces. **Ejemplo: Descargaré siempre SPOTIFY solo de su dominio oficial o desde alguna web que ofrezca descarga desde su dominio oficial**
- b. Los mensajes que tratan de dirigirte a páginas maliciosas suelen ser muy convincentes y atractivos.

6. Cuidado con lo que descargas.

- a. Descarga los ficheros de fuentes confiables.
- b. **Descarga los programas desde sus páginas oficiales.**

7. **Desconfía de los correos de remitentes desconocidos.**

- a. No responder nunca a esos mensajes.
- b. Lo más recomendable es eliminarlos directamente.



spotify descargar

Aproximadamente 31.200.000 resultados (0,51 segundos)

Anuncio - [www.spotify.com/](#) -
Prueba Spotify® Premium - Gratis los primeros
 Luego, paga solo 9,99 €/mes. Tu álbum favorito suena aun mejor c...
 Pásate a Premium hoy para escuchar música sin anuncios y saltar
 Playlists seleccionadas. Descubre nueva música. +50 millones de

Escucha gratis en Spotify
 Escucha tus Canciones Favoritas
 Más, Gratis. Regístrate hoy.

Spotify® Estudiantes
 Spotify® Premium: 50 % de descuento
 1 mes gratis. Después, 4,99 €/mes.

[www.spotify.com](#) > download > windows -
Descargar para Windows - Spotify
 Visita la Microsoft Store para **descargar**. Ponles música también a
Spotify en teléfono o tablet es gratis, fácil ...

[support.spotify.com](#) > download-the-spotify-player -
Descargar la app - Spotify
 28 nov 2019 — **Descargar** la app es totalmente gratis y no se cobr...
 funciones ... Descubre cómo **descargar Spotify** en cada dispositi...

[www.spotify.com](#) > download > other -
Descarga gratis para tu plataforma - Spotify
Descargar Spotify. Mac OS X (Actual | 10.5). Windows - iOS; And...
Spotify para otras plataformas. Linux - Windows Mobile ...

[spotifyuptodown.com](#) > ... > Sonido > Spotify -
descargar spotify gratis (android)
Spotify para Android es una excelente aplicación que transferirá to...
 imprescindible programa de ordenador a tu teléfono móvil favorito.
 ★★★★★ Valoración: 4,3 - 183 votos - Gratis - Android - Multimedi...

[spotifyuptodown.com](#) > ... > Streaming de audio -
Spotify 1.1.46.916 para Windows - Descargar
Descargar la última versión de **Spotify** para Windows. Escucha a...
 por streaming. Imagina tener uno de los mayores catálogos de ...
 ★★★★★ Valoración: 3,8 - 16 votos - Gratis - Windows - Multimedi...

[spotifysoftonic.com](#) > Windows > Multimedia > Audio -
Spotify - Descargar
Spotify, **descargar** gratis. Spotify última versión: Aplicación gratui...
 streaming. Spotify es una aplicación diseñada para escuchar ...

PHOTOSHOP descargar

Aproximadamente 40.300.000 resultados (0,35 segundos)

Anuncio - [www.adobe.com/](#) -
Descarga Adobe Photoshop® - Versión de prueba gratuita
 Cientos de tutoriales y plantillas para crear lo que quieras. ¡Prueba gratuita Barra herr...
 personalizada. Diseño mesas de trabajo. Impresión en 3D. Búsqueda en aplicaciones.
Black Friday: 20% de descuento en Adobe Creative Cloud - Válido desde el 16 nov has

¿Qué es Adobe Photoshop CC?

¿Por qué Adobe Photoshop CC y no CS7?

¿Es Photoshop CC gratis?

[www.malavida.com](#) > ... > Editores de imagen -
Photoshop CC 2020 22.0.0.35 - Descargar para PC Gratis
 6/10 (27918 votos) - **Descargar Photoshop** para PC Última Versión Gratis. Disfruta en...
 ordenador de las exhaustivas funciones y características del mejor ...
 Photoshop Android - Photoshop iPhone - Trucos Photoshop - Photoshop Portable

[adobe-photoshop-express-windows-10.softonic.com](#) > ... -
Descargar Adobe Photoshop Express for Windows 10 - gratis
Descargar ahora Adobe **Photoshop** Express for Windows 10 desde Softonic: **Descarg...**
 100% segura y libre de virus. Adobe **Photoshop** Express for ...
 ★★★★★ Valoración: 7/10 - 4.961 votos - Gratis - Windows - Multimedia

[computerhoy.com](#) > Listas > Tecnología -
 4.02 VISTA PREVIA 14 jun 2020

Cómo Descargar e Instalar Photoshop CS6 PORTABLE
 YouTube - BrayanyT RD
 25 ene 2020
 Ver todo

[www.adobe.com](#) > photoshop > free-trial-download -
Photoshop gratuito | Descargar la versión completa de Adobe
Descarga la versión completa de Adobe **Photoshop** gratis. Crea y mejora tus fotos, imá...
 obras en 3D y mucho más. Comienza a usar la versión de prueba ...

[adobe-photoshop.softonic.com](#) > ... > Fotografía -
Descargar Adobe Photoshop CC - última versión
Descargar ahora Adobe **Photoshop** CC para Windows desde Softonic: **Descarga** grati...
 segura y libre de virus. Adobe **Photoshop** CC última versión 2020 ...
 ★★★★★ Valoración: 7/10 - 37.606 votos - Gratis - Windows - Multimedia

En los buscadores, daremos preferencia siempre a los sitios web oficiales de la aplicación (captura 1) o del fabricante (captura 2).

IMPORTANTE: Nos fijaremos en el DOMINIO PRINCIPAL:

SINTAXIS: subdominio.dominioprincipal.extension

¿Qué opciones crees que serán las más LIBRES DE MALWARE en estos ejemplos?

descargar EXCEL

Aproximadamente 53.900.000 resultados (0,42 segundos)

excel.descargar.es ▾

Microsoft Excel | Descargar Gratis

Excel ayuda en tareas estadísticas y contables para asistir a los usuarios en cualquier proyecto que requiera el manejo de grandes volúmenes de información.

microsoft_excel.es.downloadastro.com ▾

Microsoft Excel - Última versión 2020. Descargar gratis

27 jun 2019 — **Descarga** gratuita de Microsoft **Excel** 2019 16.0.6742.2048 . Obtén la nueva versión de Microsoft **Excel**. Programa de hoja de cálculo con ...

excel-online.softonic.com > ... > Ofimática ▾

Excel Online - Descargar

22 mar 2020 — **Excel** Online, **descargar** gratis. **Excel** Online última versión: Crea increíbles hojas de cálculo en línea de forma gratuita. **Excel** Online es una ...

microsoft-excel-viewer.softonic.com > ... > Ofimática ▾

Descargar Microsoft Excel Viewer gratis - última versión

Descargar ahora Microsoft **Excel** Viewer para Windows desde Softonic: **Descarga** gratis, 100% segura y libre de virus. Microsoft **Excel** Viewer última versión ...

★★★★★ Valoración: 7/10 - 5.200 votos - Gratis - Windows - Negocios/Productividad

descargar VLC

Aproximadamente 2.840.000 resultados (0,54 segundos)

www.videolan.org > vlc > index.es.html ▾

Descarga oficial del Reproductor multimedia VLC, el mejor ...

... y framework multiplataforma gratuito y de código abierto que reproduce la mayoría de archivos multimedia y varios protocolos de emisión. **Descargar VLC**.

Windows

... y framework multiplataforma gratuito y de código abierto que ...

Más resultados de videolan.org >

www.videolan.org ▾

VLC: Sitio oficial - ¡Soluciones multimedia libres para todos ...

... y framework multiplataforma gratuito y de código abierto que reproduce la mayoría de archivos multimedia y varios protocolos de emisión. **Descargar VLC**.

vlc-media-player.uptodown.com > windows > descargar ▾

descargar vlc media player gratis (windows)

VLC Media Player es un reproductor multimedia multiplataforma y de código abierto distribuido bajo licencia GPL que permite reproducir prácticamente todos ...

★★★★★ Valoración: 4,3 - 76 votos - Gratis - Windows

vlc-media-player.uptodown.com > ... > Reproductores ▾

VLC Media Player 3.0.11 para Windows - Descargar

Descargar la última versión de **VLC** Media Player para Windows. Potente reproductor multimedia y servidor de streaming. **VLC** Media Player es un reproductor ...

★★★★★ Valoración: 4,3 - 76 votos - Gratis - Windows

vlc-media-player.softonic.com > ... > Multimedia > Vídeo ▾

Descargar VLC media player gratis - última versión

Descargar ahora **VLC** media player para Windows desde Softonic: **Descarga** gratis, 100% segura y libre de virus. **VLC** media player última versión 2020, más ...

★★★★★ Valoración: 8/10 - 83.962 votos - Gratis - Windows - Multimedia

descargar FIREFOX

Aproximadamente 37.600.000 resultados (0,33 segundos)

www.mozilla.org > es-ES > firefox > new ▾

Descarga Navegador Firefox — Rápido, privado y gratis — de ...

Descarga Firefox, un navegador web gratuito proporcionado por Mozilla, una organización sin ánimo de lucro dedicada a la salud de internet y a la privacidad.

Descargar Mozilla Firefox para...

Descarga Mozilla Firefox, el navegador gratuito desarrollado ...

Más resultados de mozilla.org >

www.mozilla.org > es-ES > firefox > all

Descarga el navegador Navegador Firefox en español - Mozilla

Elige qué navegador **Navegador Firefox** quieres **descargar** en tu idioma. Todo el mundo merece tener acceso a Internet, y tu idioma nunca debería ser una ...

mozilla-firefox.softonic.com > ... > Navegadores web ▾

Descargar Mozilla Firefox gratis - última versión

Descargar ahora **Mozilla Firefox** para Windows desde Softonic: **Descarga** gratis, 100% segura y libre de virus. **Mozilla Firefox** última versión 2020, más de ...

★★★★★ Valoración: 8/10 - 43.881 votos - Gratis - Windows - Navegador de Internet

¿Qué opciones crees que serán las más LIBRES DE MALWARE en estos ejemplos?

descargar EXCEL

Aproximadamente 53.900.000 resultados (0,42 segundos)

[excel.descargar.es](#)

Microsoft Excel | Descargar Gratis

Excel ayuda en tareas estadísticas y contables para asistir a los usuarios en cualquier proyecto que requiera el manejo de grandes volúmenes de información.

[microsoft_excel.es.downloadastro.com](#)

Microsoft Excel - Última versión 2020. Descargar gratis

27 jun 2019 — Descarga gratuita de Microsoft Excel 2019 16.0.6742.2048. Obtén la nueva versión de Microsoft Excel. Programa de hoja de cálculo con ...

[excel-online.softonic.com](#) Ofimática

Excel Online - Descargar

22 mar 2020 — Excel Online, descargar gratis. Excel Online última versión: Crea increíbles hojas de cálculo en línea de forma gratuita. Excel Online es una ...

[microsoft-excel-viewer.softonic.com](#) Ofimática

Descargar Microsoft Excel Viewer gratis - última versión

Descargar ahora Microsoft Excel Viewer para Windows desde Softonic: Descarga gratis, 100% segura y libre de virus. Microsoft Excel Viewer última versión ...

★★★★★ Valoración: 7/10 - 5.200 votos - Gratis - Windows - Negocios/Productividad

descargar VLC

Aproximadamente 2.840.000 resultados (0,54 segundos)

[www.videolan.org](#) > vlc > index.es.html

Descarga oficial del Reproductor multimedia VLC, el mejor ...

... y framework multiplataforma gratuito y de código abierto que reproduce la mayoría de archivos multimedia y varios protocolos de emisión. **Descargar VLC.**

Windows

... y framework multiplataforma gratuito y de código abierto que ...

Más resultados de videolan.org >

[www.videolan.org](#)

VLC: Sitio oficial - ¡Soluciones multimedia libres para todos ...

... y framework multiplataforma gratuito y de código abierto que reproduce la mayoría de archivos multimedia y varios protocolos de emisión. **Descargar VLC.**

[vlc-media-player.uptodown.com](#) > windows > descargar

descargar vlc media player gratis (windows)

VLC Media Player es un reproductor multimedia multiplataforma y de código abierto distribuido bajo licencia GPL que permite reproducir prácticamente todos ...

★★★★★ Valoración: 4,3 - 76 votos - Gratis - Windows

[vlc-media-player.uptodown.com](#) > > Reproductores

VLC Media Player 3.0.11 para Windows - Descargar

Descargar la última versión de VLC Media Player para Windows. Potente reproductor multimedia y servidor de streaming. VLC Media Player es un reproductor ...

★★★★★ Valoración: 4,3 - 76 votos - Gratis - Windows

[vlc-media-player.softonic.com](#) > > Multimedia > Video

Descargar VLC media player gratis - última versión

Descargar ahora VLC media player para Windows desde Softonic: Descarga gratis, 100% segura y libre de virus. VLC media player última versión 2020, más ...

★★★★★ Valoración: 8/10 - 83.962 votos - Gratis - Windows - Multimedia

descargar FIREFOX

Aproximadamente 37.600.000 resultados (0,33 segundos)

[www.mozilla.org](#) > es-ES > firefox > new

Descarga Navegador Firefox — Rápido, privado y gratis — de ...

Descarga Firefox, un navegador web gratuito proporcionado por Mozilla, una organización sin ánimo de lucro dedicada a la salud de internet y a la privacidad.

Descargar Mozilla Firefox para...

Descarga Mozilla Firefox, el navegador gratuito desarrollado ...

Más resultados de mozilla.org >

[www.mozilla.org](#) > es-ES > firefox > all

Descarga el navegador Navegador Firefox en español - Mozilla

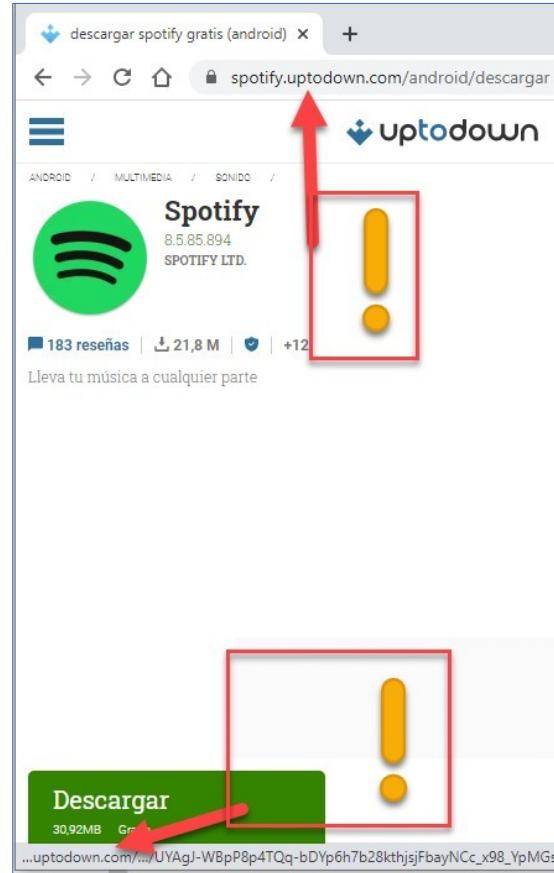
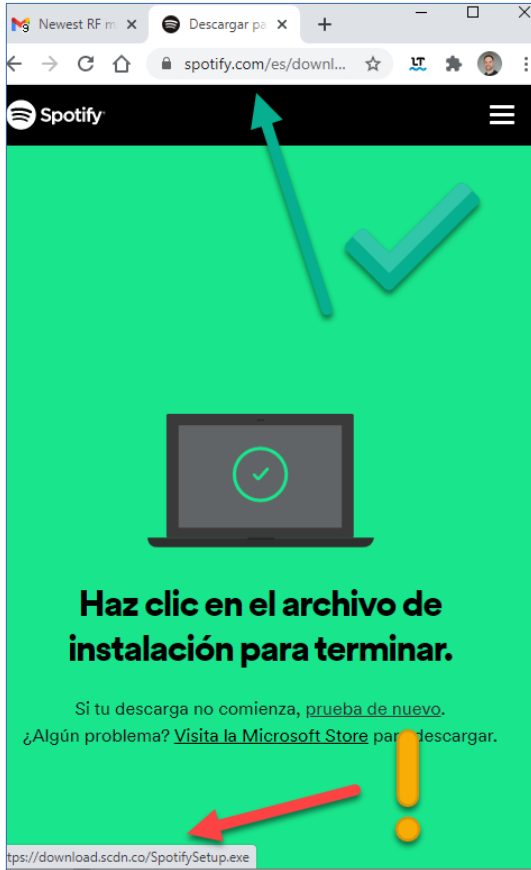
Elige qué navegador Navegador Firefox quieres descargar en tu idioma. Todo el mundo merece tener acceso a Internet, y tu idioma nunca debería ser una ...

[mozilla-firefox.softonic.com](#) > > Navegadores web

Descargar Mozilla Firefox gratis - última versión

Descargar ahora Mozilla Firefox para Windows desde Softonic: Descarga gratis, 100% segura y libre de virus. Mozilla Firefox última versión 2020, más de ...

★★★★★ Valoración: 8/10 - 43.881 votos - Gratis - Windows - Navegador de Internet



Descarga software SIEMPRE desde su dominio oficial

MUY IMPORTANTE:
El dominio oficial de la aplicación
(o del fabricante)
debe aparecer en la
barra de título o en
la barra de estado

Ejemplo: Descargaré siempre SPOTIFY

- a) Desde su dominio oficial
- b) Desde alguna web que ofrezca
descarga desde su dominio oficial

Cualquier otra combinación: **tiene riesgo de MALWARE.**

2. PRÁCTICAS DE SEGURIDAD

8. No abras ficheros adjuntos sospechosos. **FUENTE nº1 MALWARE**
 - a. Si proviene de un conocido pero no lo has solicitado, asegúrate antes de que el envío fue intencionado.
 - b. Si proviene de un desconocido, no lo abras nunca. **Abre y lee el email, pero NUNCA el adjunto.**
9. Piensa antes de publicar en las redes sociales.
 - a. El valor de tu información privada puede ser muy alto para aquellos que quieren utilizarla con fines ilícitos.
 - b. Una vez un contenido está publicado, es muy difícil eliminarlo de la red.
10. Cuidado con la wifi gratuita.
 - a. Cualquiera se puede conectar y dejar software malicioso en la red.
 - b. No te conectes ni realices operaciones delicadas, como entrar a tu banca electrónica.



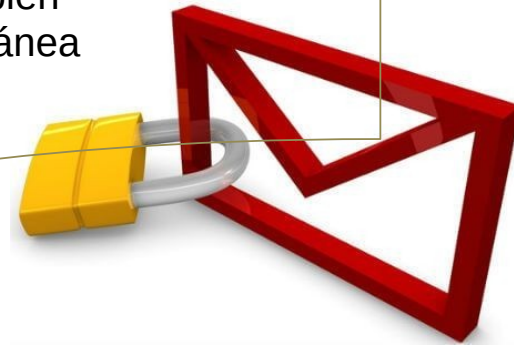
Índice

1. Introducción
2. Prácticas de seguridad recomendadas
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

FUENTE nº1 de MALWARE

- El correo electrónico es un fantástico sistema de comunicación y de intercambio de información.
- Lo podemos utilizar en el ordenador y en el móvil, nos podemos conectar a él desde muchos sitios únicamente disponiendo de una conexión a internet y un navegador.
- Pero al mismo tiempo se ha convertido en una vía de entrada de información falsa, de estafas, de virus, de publicidad, etc
- Los bulos (HOAX) no sólo existen en el ámbito del e-mail. También hay HOAX que circulan en sistemas de mensajería instantánea Whatsapp o en redes sociales.

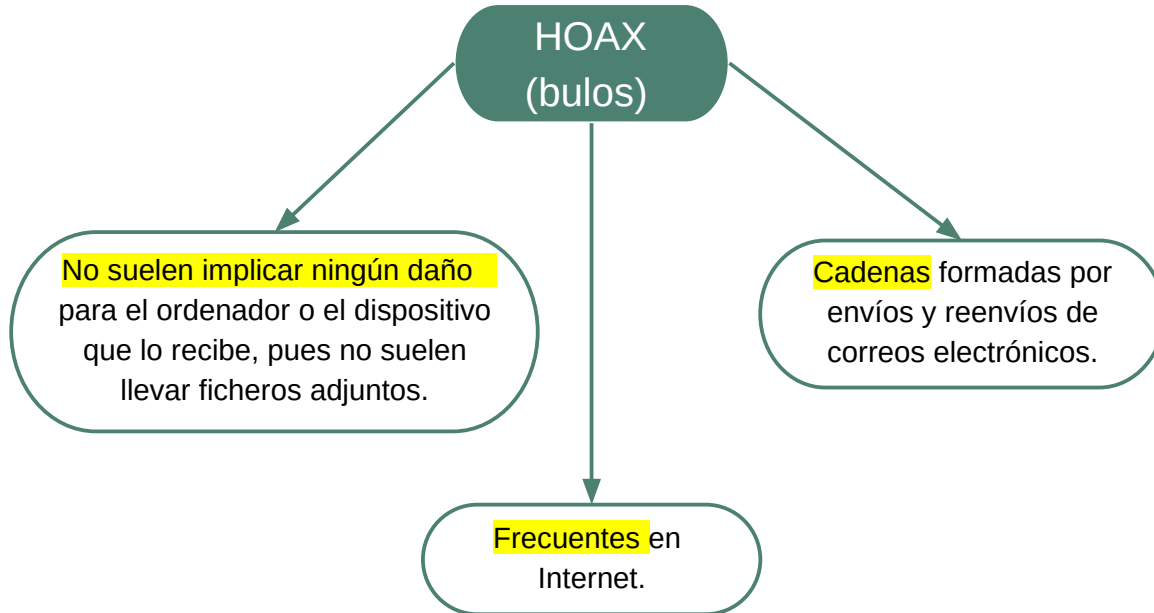


Índice

1. Introducción
2. Prácticas de seguridad recomendadas
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.1. Hoax (bulos)



3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.1. Hoax (bulos)

¿Cómo funcionan?

- Difunden supuestas **noticias sensibles** → personas con necesidad de una donación de órganos, ...
- Intento de difusión de noticias falsas y rumores (bulos).
- Regalos por contestar o reenviar a "X" amigos, o años de mala suerte si no lo haces.

¿Qué pretenden?

- Difamar o fomentar la mala imagen de empresas o personas conocidas.
- Sobrecargar servidores de correo o bloquear centralitas telefónicas.
- Difundir noticias falsas.
- Obtener direcciones de correo para generar spam.

¿Cómo detectarlos?

- No tienen fechas para que puedan ser reutilizados.
- Temas atractivos (famosos, regalos, peticiones de ayuda, etc.)
- Suelen ser anónimos.
- Solicitan el reenvío del correo.

Borrarlos y no difundirlos.

Avisar al remitente si es conocido.

Índice

1. Introducción
2. Prácticas de seguridad recomendadas
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.2. SPAM (correo basura)

¿Qué es SPAM?

- SPAM” era una marca de carne enlatada que los soldados norteamericanos recibían por correo de sus familiares durante la Segunda Guerra Mundial → Sketch Monty Phyton.
- Son mensajes no solicitados, principalmente de tipo publicitario, y enviados de forma masiva
- La forma de envío más utilizada es el correo electrónico, pero también puede presentarse por programas de mensajería instantánea o redes sociales
- La mayor parte del spam que circula por correo electrónico está escrito en inglés, y se origina en Estados Unidos y Asia, aunque ya se está extendiendo al español.



3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.2. SPAM (correo basura)

¿Cómo funcionan?

- Ofertas y promociones de empresas reales → publicidad no solicitada.
- Muchas veces engañosa y falsa.
- Estrategia → tentar con ofertas de artículos a precios atractivo.
- Se juega con la curiosidad (enlaces a videos divertidos, o de famosos en situaciones comprometidas).

¿Qué pretenden?

- Nuevas direcciones de correo
- Infectar otros ordenadores para que reenvíen spam sin saberlo.
- Enlaces a videos en redes sociales, o clic “me gusta” → generan ingresos a los sus propietarios.
- No responder, ni pinchar en los enlaces o adjuntos
- El spammer puede usar o vender.

¿Cómo detectarlos?

- Servicios públicos (Gmail, Hotmail, Yahoo! ...) incluyen filtros contra el spam
- Consejo → desconfiar de email de desconocidos u entidades sin relación. Y, por supuesto, de los chollos.
- No existe interés en el receptor, sólo que alguno adquiriera los productos o se infecte.
- Si objetivo = destinatario → SCAM

Índice

1. Introducción
2. Prácticas de seguridad recomendadas
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.2. SCAM (estafa)

¿Qué es SCAM?

Cuando el objetivo es estafar a la persona que recibe el correo electrónico.

El remitente pretende engañar al destinatario → tiene un objetivo muy claro: su dinero.

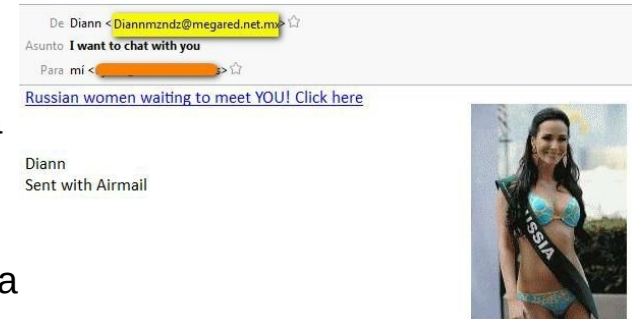


3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.2. SCAM (estafa) → ¿Cómo funciona?

Estrategia → Necesidad económica, codicia o ingenuidad.

- Loterías o sorteos. Premiado en un sorteo o lotería, en el que no ha participado. Suelen incluir logotipos y marcas para dar una apariencia oficial.
- Novias extranjeras. Correos de mujeres extranjeras, que buscan pareja, o que quieren huir de su país. Tras ganarse la confianza solicitan dinero para un viaje que no se realizará nunca.
- Cartas nigerianas. Correos de personas que viven en países con problemas políticos o bélicos, y que necesita sacar una cantidad importante de dinero de su país, para lo que solicita nuestra ayuda.



3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.2. SCAM (estafa) → ¿Cómo funciona?

- Ofertas de empleo falsas. Condiciones laborales ventajosas, pero piden hacer un ingreso para optar a ellos.
- Muleros. Correos que buscan captar muleros para blanquear dinero obtenido en actividades ilegales. Ofrecen trabajo muy cómodo, desde casa (gestionar transferencias de dinero entre cuentas de supuestos clientes utilizando nuestra cuenta como paso intermedio) → Comisión fija sobre el dinero transferido.

OJO!!! formará parte de la trama de blanqueo de dinero → consecuencias legales.

¡oferta del trabajo!

te ofrecemos una posibilidad de ganar dinero de una manera simple. puedes hacerlo sin dejar tu trabajo. solo tienes que encontrar 2 - 3 horas al día en tu horario 1 - 2 veces a la semana.

resumen de la actividad:

1. hacemos una transferencia de 3.000 eur a tu cuenta bancaria.
2. al recibir el ingreso sacas el dinero en efectivo.
- 3 ya has ganado 20 por ciento de la cantidad transferida - te queda 600 eur!
4. el resto de la cantidad - 2.400 eur lo entregas a nuestro agente.

la cantidad del ingreso y la frecuencia se pueden aumentar o reducir según tu deseo.

esta actividad es absolutamente legal y no viola ninguna ley de españa o de unión europea.

si nuestra propuesta te interesa confirmalo a la dirección **es@{ _text5}**. te contactaremos en cuanto antes y contestaremos tus preguntas.

¡ten prisa, la cantidad de vacancias está limitada!

nuestra organización le pide perdón si este mensaje le ha molestado. su dirección e-mail se ha encontrado en las fuentes de información abiertas en red. si este e-mail le ha llegado por error y si quiere eliminar su dirección electrónica de nuestra base del envío de publicidad mándenos una carta electrónica vacía a la dirección siguiente: **del@{ _text3}**. muchas gracias.

3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.2. SCAM (estafa) → ¿Qué pretenden?

- El objetivo es conseguir nuestro dinero.
- Más tarde o más temprano, nos solicitarán un envío de dinero.
- En el caso de los muleros, lo que buscan es utilizar nuestras cuentas bancarias para realizar los movimientos de blanqueo de capitales.



3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

3.2. SCAM (estafa) → ¿Cómo detectarlos?

- Utilizar el sentido común para detectar ofertas sospechosas.
- Normalmente, utilizan un lenguaje confuso y ambiguo, y en muchas ocasiones contienen errores sintácticos u ortográficos.
- Utilizan cuentas de correo gratuitas.
- Los correos que envían son plantillas modelo y apenas están personalizados.
- En algún momento solicitan un envío de dinero con cualquier excusa (a través de Western Union o Money Gram)
- El correo nos llega sin haber iniciado un contacto previo: una oferta de trabajo que no hemos demandado, un premio de una lotería en la que no hemos participado, etc.
- En muchas ocasiones, la empresa que nos ofrece trabajo, la chica que nos quiere conocer o el premio que hemos ganado están ubicados fuera de España.

3. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL e-MAIL

Consejos finales

El correo electrónico es una fantástica herramienta, que nos ofrece muchas posibilidades, tanto en el trabajo como en el ámbito privado, pero hay que ser precavidos en su uso.

Con unas sencillas pautas podemos evitar los problemas asociados a este tipo de correos:

- Seamos precavidos. Si suena demasiado bueno para ser verdad, es que probablemente sea mentira.
- No respondamos a estos correos. Al hacerlo estamos diciendo que detrás de esa dirección de email estamos nosotros.
- Jamás proporcionemos datos personales ni datos bancarios.
- Nunca pinchemos en los enlaces que nos proporcionan, ni visitemos ninguna web sugerida en el correo.



Índice

1. Introducción
2. Prácticas de seguridad recomendadas
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

4. IMPORTANCIA DE LA ADOPCIÓN DE MEDIDAS DE SEGURIDAD.

- Existen piratas informáticos maliciosos (**crackers que no hackers**), que buscan tener acceso a la red para modificar, sustraer o borrar datos.
- Según los expertos, más de 70% de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno de las organizaciones, ya que conoce la información sensible de las mismas.
- Esquemas ineficientes de seguridad para proteger los recursos informáticos de las amenazas actuales pues es algo relativamente nuevo.
- La violación de los sistemas provoca la pérdida o modificación de los datos sensibles de la organización, lo que puede representar daños de miles o millones de dólares.
- A nivel individual, también nosotros debemos informarnos bien de cómo funcionan nuestros dispositivos electrónicos y de cómo hacer un uso seguro de los mismos

4. IMPORTANCIA DE LA ADOPCIÓN DE MEDIDAS DE SEGURIDAD.



- Pertenece al INCIBE y proporciona la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.
- Su objetivo es reforzar la confianza en el ámbito digital a través de la formación en materia de ciberseguridad y para ello tienen un portal web con mucha información útil: <https://www.osi.es/>.



Centro de Seguridad TIC de la Comunitat Valenciana (junio 2007). Ofrece servicios dentro de la Comunitat Valenciana, con vocación de servicio público, sin ánimo de lucro, por lo que sus servicios se ofrecen gratuitamente.

- Servicios Reactivos → petición previa.
- Servicios Preventivos → anticipación.
- Servicios de Valor Añadido → formación y/o asesoría.

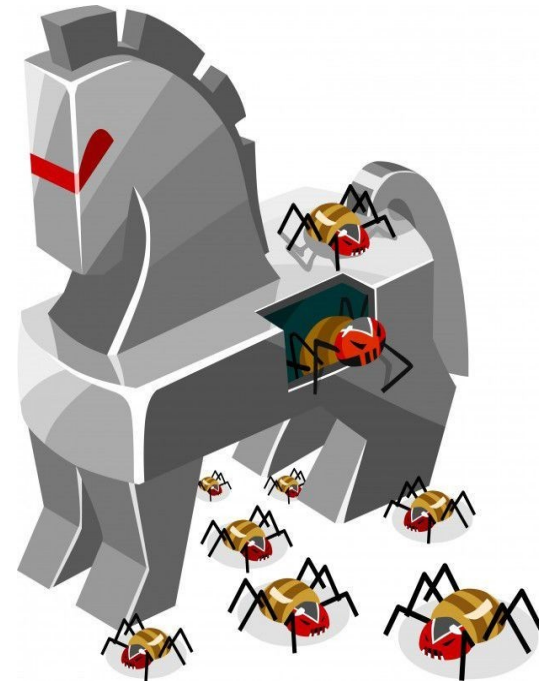
Índice

1. Introducción
2. Prácticas de seguridad recomendadas
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

5. TÉCNICAS HABITUALES DE FRAUDE.

5.1 Troyanos

- Tipo de malware cuyo principal propósito → **dar acceso remoto** a un sistema (Caballo de Troya).
- Troyano = programa oculto dentro de otro, que ejecuta comandos furtivamente y abre el acceso al ordenador (puerta trasera).
- Un Troyano crea una infracción de seguridad para usuarios externos accedan áreas protegidas de la red.
 - Eliminar/destruir información del disco duro.
 - Capturar y reenviar datos confidenciales a una dirección externa (ej. contraseñas introducidas por teclado)
 - Abrir puertos de comunicaciones, permitiendo que un posible intruso controle nuestro ordenador de forma remota.
- Muy utilizados por los ciberdelincuentes para robar datos bancarios.



5. TÉCNICAS HABITUALES DE FRAUDE.

5.1 Troyanos

Evolución informática de los troyanos

- Se concibieron como una herramienta para causar el mayor daño posible en el equipo infectado (formatear ordenador, eliminar archivos del sistema, ...).

No tuvieron mucha repercusión porque no se propagaban por sí mismos.

Un tipo de troyano son los **Backdoors** o puerta trasera. Un troyano de estas características, le permite al atacante conectarse remotamente al equipo infectado. Las conexiones remotas son comúnmente utilizadas en informática y la única diferencia entre estas y un backdoor es que en el segundo caso, la herramienta es instalada sin el consentimiento del usuario.

- Actualmente gracias a Internet, son una herramienta para robar datos bancarios, nombres de usuario y contraseñas, información personal, etc. → Creación de una nueva categoría de malware: los troyanos bancarios y el Spyware.

5. TÉCNICAS HABITUALES DE FRAUDE.

5.1 Troyanos

¿Cómo podemos protegernos de los troyanos?

- Evita la descarga de contenidos desde páginas desconocidas o de dudosa reputación.
- Vigila las descargas realizadas desde aplicaciones P2P.
- Mantén actualizado tu antivirus. Si no dispones de antivirus, instala cualquiera de los antivirus gratuitos y estarás protegido frente a estas amenazas.
- Haz un análisis gratuito de tu ordenador y comprueba si está libre de troyanos.

Índice

1. Introducción
2. Prácticas de seguridad recomendadas
3. Problemas de seguridad y protección en el correo electrónico
 - 3.1. Hoax
 - 3.2. SPAM
 - 3.3. SCAM
4. Importancia de la adopción de medidas de seguridad.
 - 4.1. OSI - Oficina de Seguridad del Internauta
 - 4.2. CSIRT-CV
5. Técnicas habituales de fraude: troyanos y phishing
 - 5.1. TROYANOS
 - 5.2. Phishing
6. BIBLIOGRAFÍA

5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 1/13

- Phishing (proviene de la palabra inglesa "fishing" pesca).
- Envío por parte de un delincuente de un correo electrónico a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada.
- Contienen algún enlace a una página falsa que suplanta la identidad de una empresa o servicio en la que, si introducimos nuestros datos, éstos pasarán directamente a manos del estafador.
- Cada vez más, se están detectando casos de este fraude con el mismo objetivo, a través de otros medios como pueden ser los mensajes intercambiados a través de aplicaciones de mensajería instantánea, mensajes en redes sociales o SMS.



5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 2/13

¿Qué características tienen en común los correos de phishing?

Utilizan argumentos ingeniosos relacionados con la seguridad de la entidad o el adelanto de algún trámite administrativo para justificar la necesidad de facilitar sus datos personales.

Excusas
frecuentes

- Problemas de carácter técnico.
- Detecciones de fraude y urgente incremento del nivel de seguridad.
- Nuevas recomendaciones de seguridad para prevención del fraude.
- Cambios en la política de seguridad de la entidad.
- Promoción de nuevos productos.
- Premios, regalos o ingresos económicos inesperados.
- Accesos o usos anómalos a tu cuenta.
- Inminente desactivación del servicio.
- Falsas ofertas de empleo.

5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 3/13

¿Qué características tienen en común los correos de phishing?

Trata de forzar a tomar una decisión inmediata
→ consecuencias negativas
(ej. denegación de acceso al servicio o pago de una multa económica)

Se generan a través de herramientas automáticas → faltas ortográficas y errores gramaticales.

5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 4/13

¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

1 Bancos y cajas

Excusas:

- cambio en la normativa del banco,
- cierre incorrecto de la sesión del usuario,
- mejoras en las medidas de seguridad,
- detectada intrusión en sus sistemas de seguridad,
- bloqueo de la cuenta por motivos de seguridad, etc.

Objetivo: robar números de tarjetas de crédito, tarjetas de coordenadas, PIN secreto, etc.

The image shows a simulated phishing interface. On the left, there are two grids of numbers. The first grid is titled 'Clave de Seguridad' and contains numbers 1 through 6. The second grid is titled 'Tarjeta de Coordenadas -primeros 24 numeros-' and contains numbers 1 through 24. On the right, there is a form with the following fields:

- Nombre del titular :
- D.N.I. :
- Número de tarjeta :
- Fecha de vencimiento : /
- CSC :
- PIN :
- Usuario :
- Clave :
- Firma electrónica :

At the bottom right, there is a button labeled 'Completar'.

5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 5/13

¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

2 Pasarelas de pago online (PayPal, Mastercard, Visa, etc.)

Excusas:

- Cambio en la normativa del servicio
- Cierre incorrecto de la sesión del usuario.
- Mejoras en las medidas de seguridad.
- Detectada intrusión en sus sistemas de seguridad, etc.

Objetivo: principalmente robar datos bancarios.

Update of your account Informations

Dear PayPal User,

We're constantly working to make PayPal safer, simpler and more convenient for you. This means that from time to time we have to update our customers informations to make sure that they are safe and they can make safty online payments.

What do I need to do?

[Click here](#) to sign in to your account and update your informations to make sure that your account is safe and your payment are secure .

If you have any problems contact our support for more informations.

Sincerely,

PayPal

5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 6/13

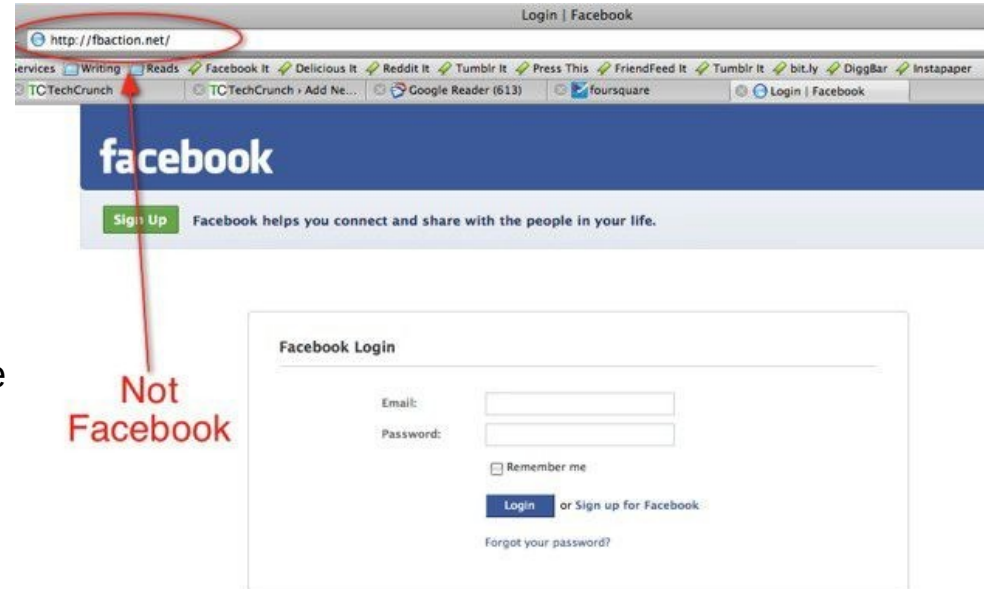
¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

3 Redes sociales (Facebook, Twitter, Tuenti, Instagram, LinkedIn, etc.)

Excusas:

- Alguien te ha enviado un mensaje privado.
- Se han detectado conexiones extrañas en la cuenta.
- Por motivos de seguridad es necesario que se cambien las claves, etc.

Objetivo: robar cuentas de usuarios, obtener sus datos privados y suplantar su identidad.



5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 7/13

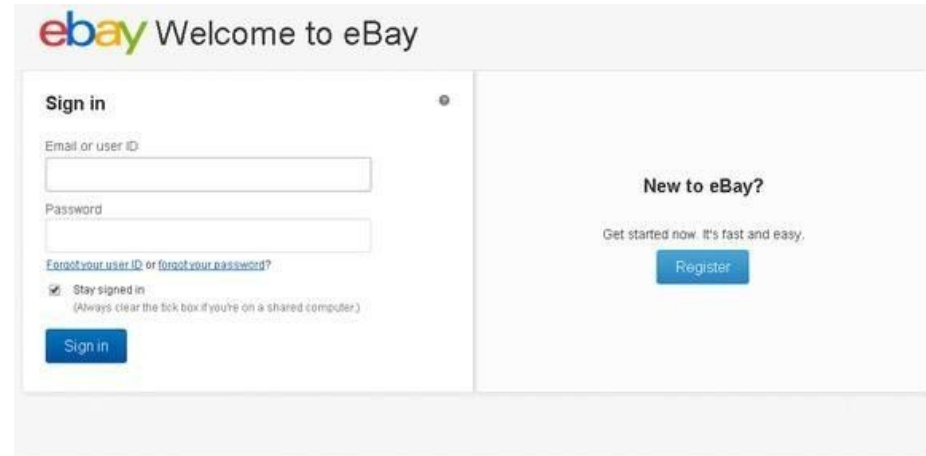
¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

4 Páginas de compraventa y subastas (Amazon, eBay, etc)

Excusas:

- Problemas en la cuenta del usuario.
- Detectados movimientos sospechosos.
- Actualización de las condiciones del uso del servicio, etc.

Objetivo: robar cuentas de usuarios y estafar económicamente al usuario



The image shows a screenshot of the eBay login page. On the left, there is a 'Sign in' section with fields for 'Email or user ID' and 'Password', a 'Forgot your user ID or forgot your password?' link, a 'Stay signed in' checkbox, and a 'Sign in' button. On the right, there is a 'New to eBay?' section with the text 'Get started now. It's fast and easy.' and a 'Register' button. The page has a clean, white background with the eBay logo at the top left.

5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 8/13

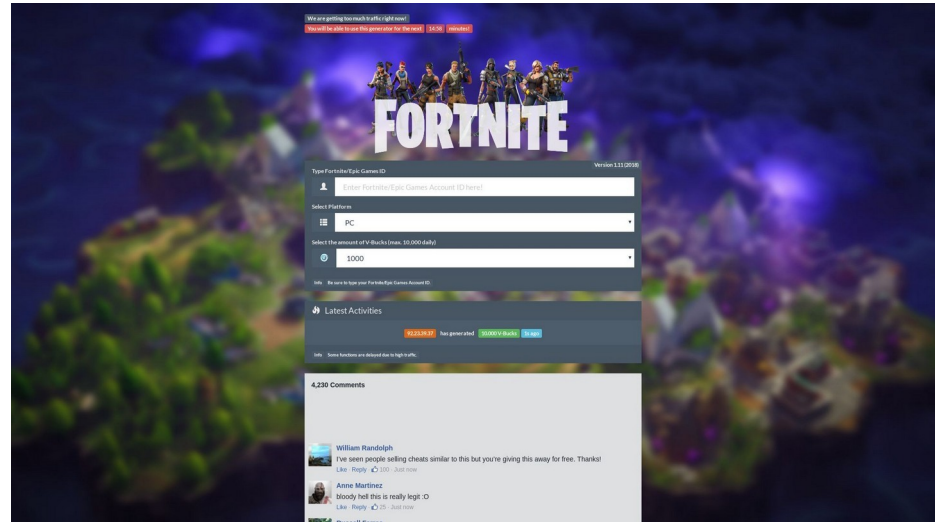
¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

5 Juegos online

Excusas:

- Problemas en la cuenta del usuario.
- Detectados movimientos sospechosos.
- Actualización de las condiciones del uso del servicio, etc.

Objetivo: robar cuentas de usuarios y estafar económicamente al usuario



5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 9/13

¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

6 Soporte técnico y de ayuda (helpdesk) de empresas y servicios (Outlook, Apple, Gmail, etc.)

Excusas:

- Confirmación de la cuenta de usuario.
- Eliminación de cuentas inactivas.
- Detectada actividad sospechosa en la cuenta.
- Se ha superado el límite de capacidad de la cuenta, etc.

Objetivo: robar cuentas y datos privados de los usuarios.

Estimado Cliente de Apple,,

Tu ID de Apple se ha desactivado temporalmente por razones de seguridad!!!

Alguien acaba de intentar iniciar sesión en tu cuenta de Apple de otra dirección IP. Por favor, confirme su identidad actual o su cuenta se desactivará debido a la preocupación que tenemos por la seguridad e integridad de la comunidad de Apple.

Para confirmar su identidad, le recomendamos que vaya a [Comprobar ahora >](#)

Saludos,
Apple



5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 10/13

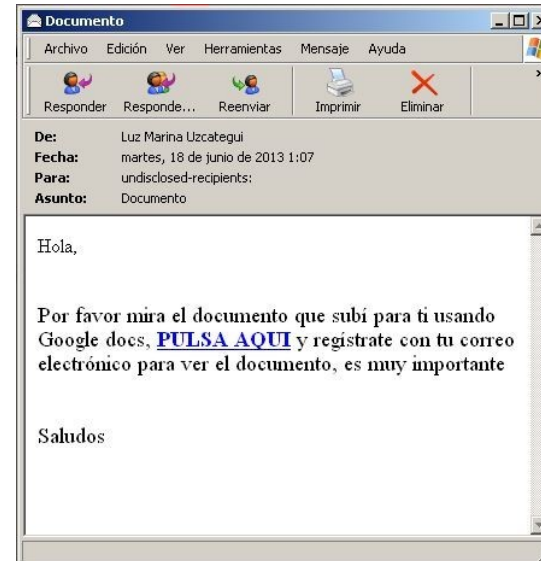
¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

7 Servicios de almacenamiento en la nube (Google Drive, Dropbox, etc.)

Excusas: Aviso de que alguien ha subido documentos a la nube para tí.

Objetivo:

- Conseguir cuentas de distintos servicios de usuarios,
- Obtener información privada.



5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 11/13

¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

8 Phishing a servicios o empresas públicas

Excusas: información sobre una notificación, una multa, etc

Objetivo:

- Infectar el ordenador.
- Robar datos privados, bancarios y estafar económicamente al usuario.

De: Agencia Tributaria [<mailto:oficina@agenciatributaria.es>]
Enviado el: martes, 14 de febrero de 2012 11:56
Asunto: Impuesto sobre NotificaciXn de Reembolso



Agencia Tributaria
14-02-2012

IMPUESTO SOBRE LA NOTIFICACIÓN DE REEMBOLSO

Estimado Contribuyente,
Después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 EUR.

Por favor, envíe la solicitud de devolución de impuestos y nos permiten 6-9 días con el fin de procesarlo.

Para acceder a su reembolso de impuestos, por favor, siga los siguientes pasos:

- Descargue el formulario de devolución de impuestos unida a este mensaje
- Abrirlo en el navegador
- Siga las instrucciones en la pantalla

Un reembolso se puede retrasar para una variedad de razones. Por ejemplo, la presentación registros inválidos o la aplicación después de la fecha límite.

5. TÉCNICAS HABITUALES DE FRAUDE.

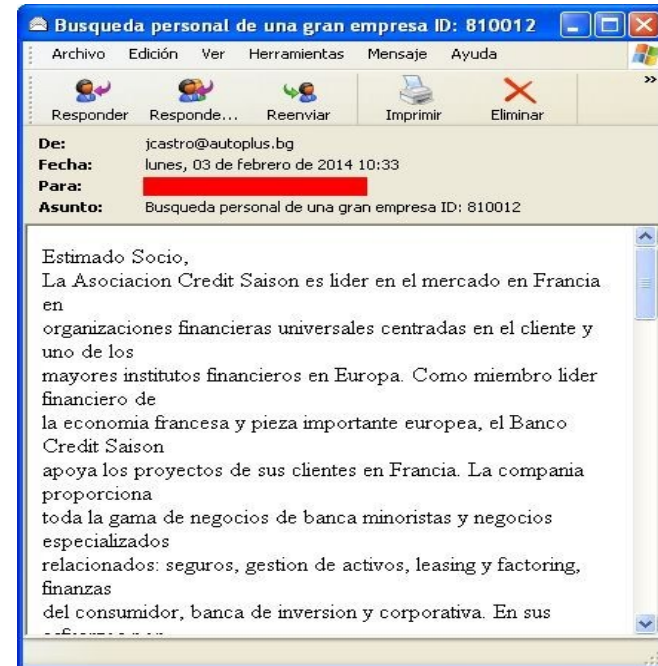
5.2 Phishing (suplantación de identidad) 12/13

¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

9 Falsas ofertas de empleo

Excusas utilizadas para engañar al usuario: puestos de trabajo.

Objetivo: robar datos privados que pueden ser utilizados posteriormente con distintos fines fraudulentos.



5. TÉCNICAS HABITUALES DE FRAUDE.

5.2 Phishing (suplantación de identidad) 13/13

¿Cómo puedes protegerte del phishing?

- Usa los filtros antispam de los clientes de correo electrónico, o utilizar herramientas específicas que bloquean el correo no deseado.
- Configura la opción antiphishing que incorporan los navegadores.
- Verifica la legitimidad del sitio web. (URL oficial sino → la están suplantando).

Has detectado un caso de phishing. ¿Qué hacer?

- No accedas a las peticiones de solicitud de información. (Si dudas → consultar con la empresa/servicio).
- No contestes en ningún caso a estos correos.
- No hagas clic en enlaces ni descargues ficheros que traiga adjuntos.
- Elimínalo y/o alerta a tus contactos.
- Algunos gestores de correo tienen la opción de informar directamente al propio gestor.
- Puedes hacer llegar los correos sospechosos al Instituto Nacional de Ciberseguridad (INCIBE) <https://www.incibe-cert.es/respuesta-incidentes>. Tienes una guía en la Oficina de Seguridad del Internauta

5. Webgrafia

1. <http://www.osi.es/es/te-ayudamos/actua-ante-el-fraude>
2. <https://es.wikipedia.org/wiki/Bulo>
3. <https://web.archive.org/web/20070105150134/http://www.rompecadenas.com.ar/hoaxes.htm>
4. <https://www.pandasecurity.com/es/security-info/>
5. <https://www.csirtcv.gva.es/>
6. <https://www.fundeu.es/recomendacion/hacker-y-cracker-diferencias-de-significado/>
7. <https://www.osi.es/>
8. <https://www.incibe.es/>
9. <https://www.incibe-cert.es/>

ACTIVIDAD

1. Comprueba si desde tu conexión a Internet ha habido algún incidente con botnets:
<https://www.osi.es/es/servicio-antibotnet>
1. Busca y comparte con tu compañeros usando el foro de la unidad alguna cadena / Spam / Phising que hayas recibido durante estas semanas del curso
3. ¡Refresca tus conocimientos en ciberseguridad! Con este cuestionario:
<https://www.osi.es/es/test-evaluacion/refresca-tus-conocimientos-enciberseguridad>
4. Contesta a este cuestionario sobre los Mitos sobre seguridad en Internet
<https://www.osi.es/es/test-evaluacion/mitos-sobre-seguridad-en-internetverdaderos-o-falsos>