CENTRE ESPECÍFIC
D´EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

UD 2

SEGURIDAD Y ÉTICA INFORMÁTICA

PARTE 2

SEGURIDAD EN INTERNET

TRATAMIENTO DE LA INFORMACIÓN Y COMPETENCIA DIGITAL (TICD)
21/22
FORMACIÓN DE PERSONAS ADULTAS / ACCESO A CFGS

Autor: Paco Aldarias
paco.aldarias@ceedcv.es
Fecha: 28-10-2021

Adaptación de los apuntes de Sergio Badal

Licencia

Nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

ÍNDICE DE CONTENIDO

UD02.2. SEGURIDAD EN INTERNET

Los virus informáticos y otras amenazas contra la seguridad informática han sido problemas muy conocidos durante un largo periodo de tiempo. El primer virus informático fue descubierto hace 20 años, y el problema ha evolucionado a una velocidad alarmante a través de los años.

Los creadores de hoy en día de software malicioso son mucho más avanzados y tienden a tener incentivos económicos y a menudo están bien organizados y usan métodos sofisticados para la propagación del malware.

1. PRÁCTICAS DE SEGURIDAD RECOMENDADAS

Podemos convertirnos en internautas seguros si nos mantenemos informados, protegemos nuestros dispositivos adecuadamente y tenemos unos buenos hábitos de uso:

1. **Utiliza un antivirus que analice todo lo que descargas**. Asegúrate de tener un antivirus instalado, mantenerlo actualizado para que reconozca el mayor número de virus, y realizar análisis regularmente de todo el sistema.
2. **Mantén el sistema operativo (SO) y el navegador actualizado**. Los virus aprovechan los defectos o agujeros del SO y navegador para infectar tus dispositivos. Como contra-medida los fabricantes corrigen los programas a través de actualizaciones. La mejor forma para estar protegido es activar las actualizaciones automáticas de tu SO, navegador, plugins del navegador y resto de aplicaciones..
3. **Cuida tus contraseñas**. Al introducirlas asegúrate de que estás en la página correcta ya que puede parecer idéntica a la legítima y tratarse de una suplantación (phishing). No utilices la misma contraseña de tu correo en diferentes servicios porque si acceden a una de tus cuentas fácilmente podrán acceder al resto. Y no compartas tus contraseñas con nadie, aunque digan que son del servicio técnico, los reales **nunca** te solicitarán las contraseñas.
4. **Confía en la web pero no seas ingenuo**. Permanece alerta, no todo lo que se dice en Internet tiene por qué ser cierto. Ante la duda contrasta la información en otras fuentes.
5. **No hagas clic en enlaces que resulten sospechoso**s. Sé precavido antes de seguir un enlace al navegar, en el correo, en la mensajería instantánea o en una red social (nadie regala dinero en Internet). Los mensajes falsos que los acompañan pueden ser muy convincentes con el fin de captar tu atención y redirigirte a páginas maliciosas.
6. **Ten cuidado con lo que descargas**. No te precipites y descargues cualquier cosa, cada día surgen nuevas amenazas y los antivirus no pueden combatirlas todas. Descarga los ficheros solo de fuentes confiables y los programas desde sus páginas oficiales, así evitarás desagradables sorpresas.
7. **Desconfía de los correos de remitentes desconocidos.** Ante la duda, es recomendable no responder a los mismos y eliminarlos directamente. Ten en cuenta también que cuanto más limites la difusión de tu cuenta de correo menos spam recibirás.

8. **No abras ficheros adjuntos sospechosos**. Si es de un conocido y no lo has solicitado, asegúrate de que realmente te lo quiso enviar. Los virus utilizan esta técnica para propagarse entre los contactos del correo, así como los contactos de la mensajería instantánea y de las redes sociales.
9. **Piensa antes de publicar**. Los servicios actuales de Internet facilitan las relaciones sociales, lo que conlleva a su vez que publiques mucha información sobre ti (datos personales, imágenes, gustos, preferencias, etc.). Dado el valor que tiene esta información, y las repercusiones negativas que puede tener su uso inadecuado por parte de otras personas, es necesario que la gestiones adecuadamente. ¡Piensa antes de publicar y controla qué información compartes!

Figura 1: Consejos sobre publicación en redes sociales de la marina americana

10. **Cuidado con la Wi-Fi gratuita**. No tienen porqué ser todas peligrosas, pero cualquiera se puede conectar y dejar software malicioso en la red. No te conectes ni realices operaciones delicadas, como entrar a tu banca electrónica.

2. PROBLEMAS DE SEGURIDAD Y PROTECCIÓN EN EL CORREO ELECTRÓNICO

El correo electrónico es un fantástico sistema de comunicación y de intercambio de información. Pero al mismo tiempo se ha convertido en una vía de entrada de información falsa, de estafas, de virus, de publicidad, etc. Los bulos no sólo existen en el ámbito del correo electrónico. También hay hoax que circulan en sistemas de mensajería instantánea como Whatsapp o en redes sociales.

2.1 Hoax

Los **bulos** o hoax (en inglés, engaño), son relativamente **frecuentes** en Internet. Son cadenas formadas por envíos y reenvíos de correos electrónicos. Generalmente no implican **ningún daño** para el ordenador o el dispositivo que lo recibe, pues no suelen llevar ficheros adjuntos.

¿Cómo funcionan?

A veces difunden supuestas noticias que intentan despertar nuestra **sensibilidad**, como personas que necesitan urgentemente una donación de órganos, o niños que precisan una transfusión.

En muchas ocasiones se trata del intento de difusión de **noticias falsas** (como los imanes cancerígenos de nevera y otros muchos), de la difusión de **rumores** o bulos sobre empresas o productos muy conocidos, o sobre noticias que tradicionalmente han generado dudas o rumores.

En otras, ofrecen **regalos** sorprendentes simplemente por contestar al correo, o por reenviarlo a diez amigos, tickets de regalo en cadenas de supermercados o, por el contrario, años de mala suerte si no los reenvías a todas tus amistades.

¿Qué pretenden?

En algunos casos **difamar** o fomentar la mala imagen de una empresa o de una persona conocida. En otros, simplemente **sobrecargar** los servidores de correo o bloquear la centralita telefónica de un hospital o de una empresa. A veces lo único que persiguen es **difundir** noticias falsas. Otro de sus objetivos es **obtener direcciones de correo** para generar spam.

¿Cómo detectarlos?

Una manera sencilla de detectarlos: introduce en un buscador en Internet el asunto del correo electrónico o alguna parte de la información que pretende divulgar, y observa los resultados. Pero:

- Normalmente no tienen fechas en su texto, para que no caduquen y puedan ser reutilizados al máximo en Internet.
- Tratan un tema que atrae al lector: noticias de famosos, regalos gratis, injusticias, peticiones de ayuda, etc.
- Suelen ser anónimos, no identifican claramente quién acredita la noticia divulgada.
- De una manera más o menos directa, solicitan el reenvío del correo .

Debemos borrarlos y no contribuir a su difusión. Si lo hemos recibido de una persona conocida, debemos informarle de ello, para evitar que siga colaborando en su reenvío.

2.2 SPAM

"SPAM" era una marca de carne enlatada que los soldados norteamericanos recibían por correo de sus familiares durante la Segunda Guerra Mundial y que usaron los Monty Phyton para hacer un número de humor en el que una señora en un bar no podía pedir ningún plato que no llevara spam.

En informática, el spam (en inglés, **correo basura**) hace referencia a **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.

¿Cómo funcionan?

En algunos casos se trata de ofertas y promociones de empresas reales. En estos casos, nos encontramos simplemente ante un caso de **publicidad no solicitada**. Pero en la mayoría de las ocasiones, además de ser publicidad no deseada y no solicitada, es publicidad **engañosa** y **falsa**.

Su estrategia más frecuente es tentar al receptor del correo con **ofertas** de artículos de lujo, medicamentos o productos ilegales a un precio muy atractivo, inferior a su precio de mercado. En otros casos se juega con la **curiosidad** de quien recibe el spam, por enlaces a videos que se anuncian como muy divertidos, o a videos de famosos en una situación comprometida.

¿Qué pretenden?

El spammer suele buscar dos cosas: **nuevas direcciones** de correo o **infectar** nuevos ordenadores que se dediquen a reenviar spam sin que sus propietarios lo sepan. En el caso de los enlaces a los videos promocionados en redes sociales, al pinchar en el enlace o al darle a "me gusta" lo que estamos haciendo es beneficiar a las personas que han creado los perfiles o páginas que se visitan, pues perciben ingresos por publicidad por las **visitas** que reciben.

No debemos responder, ni pinchar en los enlaces o adjuntos que acompañan al correo.

De hecho, el spammer puede usar él mismo las direcciones de correo que obtiene o puede vender éstas direcciones legítimas en el mercado negro y obtener dinero a cambio de ellas.

¿Cómo detectarlos?

Aunque la mayor parte de los servicios públicos de correo electrónico (Gmail, Hotmail/Outlook, Yahoo!) incluyen filtros muy eficaces contra el spam, el mejor consejo es **desconfiar** de cualquier correo electrónico que recibimos de alguien **desconocido** o de alguna empresa u organización con la que no tenemos ningún tipo de relación. Y, por supuesto, desconfiar de los chollos. Como se ha dicho siempre, "nadie regala duros a cuatro pesetas".

En el spam no existe un interés especial en el receptor del correo o del mensaje. Únicamente se espera, a través de envíos masivos, que algún destinatario adquiera los productos ofrecidos y, en el peor de los casos, su equipo resulte infectado con algún tipo de virus.

Pero a veces el objetivo sí que se centra en quien recibe el correo. En esos casos, hablamos de scam.

2.3 SCAM

Cuando el objetivo es **estafar** a la persona que recibe el correo electrónico nos encontramos ante un scam (en inglés, estafa). En este caso, el remitente del correo pretende engañar al destinatario del correo, y tiene un objetivo muy claro en la gran mayoría de los casos: su dinero.

¿Cómo funcionan?

La estrategia de estas acciones se basa en la posible **necesidad** económica que pueda tener quien lo recibe, en su **codicia** o, simplemente, en su **ingenuidad**. Existen diferentes casuísticas:

- **Loterías o sorteos**. Este tipo informan a quien lo recibe de que ha ganado una importante suma de dinero en algún sorteo o lotería, en el que curiosamente **no ha participado**. Los correos suelen incluir logotipos y marcas para dar una apariencia oficial.
- **Novias extranjeras**. En otros casos, se trata de correos electrónicos de personas, normalmente mujeres de países extranjeros, que buscan pareja, o que quieren huir del país en el que residen supuestamente por motivos de persecución política, de falta de trabajo, o por problemas sentimentales. Su objetivo es ganarse la confianza del receptor de los correos. Después de varios correos acabarán solicitando **dinero para un viaje** al país del destinatario del correo que, por supuesto, jamás llega a realizarse.
- **Cartas nigerianas**. Otro tipo de timos son correos electrónicos remitidos por una persona que vive en un país con problemas políticos o incluso bélicos, y que necesita **sacar** una cantidad importante de **dinero de su país**, para lo que solicita nuestra ayuda.
- **Ofertas de empleo falsas**. También circulan ofertas de trabajo falsos con condiciones laborales muy ventajosas, pero que **piden hacer algún ingreso** poder optar a ellos.
- **Muleros**. Un caso especialmente peligroso, es el de los correos que buscan captar muleros para **blanquear dinero** obtenido en actividades ilegales. Supuestamente, ofrecen un trabajo muy cómodo, desde casa, y en el que el trabajo a desarrollar consiste en gestionar **transferencias de dinero entre cuentas** de supuestos clientes de la empresa para la que vamos a trabajar y otras cuentas de destino, utilizando nuestra cuenta bancaria como paso intermedio. El beneficio obtenido es una comisión fija sobre el dinero transferido. Caer en este engaño es muy peligroso, pues el estafado **pasa a formar parte de la trama de blanqueo** de dinero sin ser consciente de ello y puede tener consecuencias legales.

¿Qué pretenden?

Evidentemente, 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.

¿Cómo detectarlos?

En primer lugar hay que utilizar el **sentido común**. ¿No es al menos sospechoso que nos haya tocado un premio en un sorteo en el que no hemos participado? ¿No es un poco extraño que ese señor de ese país tan remoto se ponga en contacto precisamente conmigo para que le ayude a sacar esos millones de euros que tiene? ¿Ganar 3.000 euros sin moverme de casa, tal como está el mercado de trabajo?

Pero además, hay algunos **indicios** que también nos pueden hacer sospechar de ese correo:

- 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. Normalmente las empresas utilizadas para el envío de dinero son 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**.

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.

2.3.1 Consejos finales

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.

3. IMPORTANCIA DE LA ADOPCIÓN DE MEDIDAS DE SEGURIDAD.

Es importante adoptar medidas de seguridad porque existen piratas informáticos maliciosos o **crackers** (que no hackers), que buscan tener acceso a la red para modificar, sustraer o borrar datos.

Tales personajes pueden incluso formar parte del personal administrativo o de sistemas de cualquier empresa. Según expertos en el tema, más de 70% de las violaciones e intrusiones a los recursos informáticos se realiza por el **personal interno**, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Esta situación se presenta gracias a los **esquemas ineficientes** de seguridad con los que cuentan la mayoría de las compañías, y porque no se ha planeado un esquema de seguridad eficiente que proteja los recursos informáticos de las amenazas actuales pues es algo relativamente nuevo.

El **resultado** es la violación de los sistemas, provocando 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, cuando usamos el ordenador, el smartphone o la tablet y nos conectamos a Internet, también nosotros debemos hacer lo mismo, informarnos bien de cómo funcionan dichos dispositivos electrónicos y cómo hacer un uso seguro y correcto de todos ellos para que nuestra experiencia cómo usuarios sea lo más positiva posible evitando y haciendo frente a los posibles riesgos con los que nos podamos encontrar por el camino.

3.1 OSI - Oficina de Seguridad del Internauta

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/.

3.2 CSIRT-CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007 y ofrece servicios dentro de la Comunitat Valenciana (Alicante, Castellón y Valencia), con vocación de servicio público, sin ánimo de lucro, por lo que sus servicios se ofrecen gratuitamente.

Servicios Reactivos. Se inician ante un evento o petición, siempre como reacción Los servicios reactivos son el componente central del trabajo de un CSIRT.

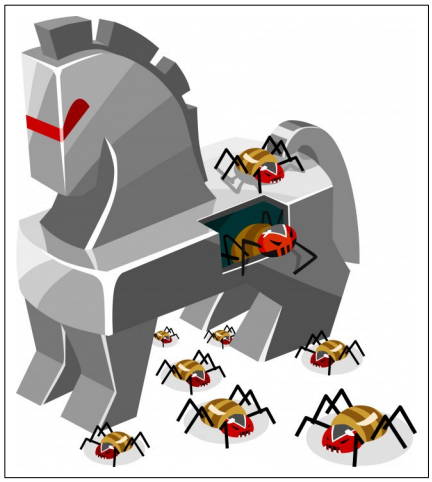
Servicios Preventivos. Ofrecen asistencia e información para ayudar a preparar, proteger y asegurar los sistemas de los miembros del área de cobertura, anticipando ataques, problemas o eventos.

Servicios de Valor Añadido. Con estos, CSIRT-CV brinda su experiencia para ayudar a mejorar la seguridad general impartiendo formación, asesoría técnica y legal en materia de seguridad.

4. TÉCNICAS HABITUALES DE FRAUDE: TROYANOS Y PHISHING

4.1 TROYANOS

Los troyanos son un tipo de malware cuyo principal propósito es dar **acceso** remoto a un sistema. Igual que el mítico caballo que usaron los griegos para introducirse en Troya sin levantar sospechas, estos programas tratan de pasar lo más desapercibidos que puedan, abriendo una puerta trasera para que un atacante remoto se introduzca en el ordenador.



Se denomina Troyano a un **programa oculto dentro de otro**, que ejecuta comandos furtivamente y que, por lo general, abre el acceso al ordenador y lo opera abriendo una puerta trasera.

Un Troyano puede crear una infracción de seguridad dentro de la **red** para que los usuarios externos puedan acceder a áreas protegidas de esa red. Pueden **eliminar ficheros** o destruir la información del disco duro. Además, son capaces de **capturar y reenviar datos** confidenciales a una dirección externa (como capturar todos los **textos** introducidos mediante el teclado o registrar las **contraseñas** introducidas por el usuario) o **abrir puertos** de comunicaciones, permitiendo que un posible intruso controle nuestro ordenador de forma remota.

Por ello, son muy utilizados por los ciberdelincuentes para robar datos bancarios.

Evolución informática de los troyanos

Los troyanos se concibieron como una herramienta para **causar el mayor daño** posible en el equipo infectado. Trataban de formatear el ordenador o eliminar archivos del sistema. Pero no tuvieron mucha repercusión ya que, en la época en la que los creadores de malware buscaban notoriedad, los troyanos no se propagaban por sí mismos. Un ejemplo de este tipo es el Autorooter.

En los últimos años, y gracias a la popularización de **Internet**, esta tendencia ha cambiado. Los ciberdelincuentes han visto en ellos la herramienta perfecta para **robar datos** bancarios, nombres de usuario y contraseñas, información personal, etc. Es decir, han dado pie a la creación de una nueva categoría de malware: los troyanos bancarios y el Spyware.

¿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 gratuítos y estarás protegido frente a estas amenazas.
- Haz un análisis gratuito de tu ordenador y comprueba si está libre de troyanos.

4.2 Phishing

Conocido como **suplantación de identidad**, consiste en el 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**.

Los correos de tipo phishing (proviene de la palabra inglesa "fishing" pesca) generalmente 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.

Cuando hablamos de phishing casi siempre lo relacionamos con el correo electrónico, aunque, cada vez más, se están detectando casos de este fraude con el mismo objetivo, pero que redirigen a una página web falsa a través de otros medios como pueden ser los mensajes intercambiados a través de aplicaciones de mensajería instantánea, mensajes en redes sociales o SMS.

¿Qué características tienen en común los correos de phishing?

Los mensajes suplantadores utilizan todo tipo de 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. Entre las excusas frecuentes nos encontramos con:

- Problemas de carácter técnico.
- Recientes 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.

Además, el correo fraudulento tratará de forzar al usuario a tomar una decisión de forma casi inmediata **advirtiendo de consecuencias negativas** como por ejemplo la denegación de acceso al servicio correspondiente o el pago de una multa económica.

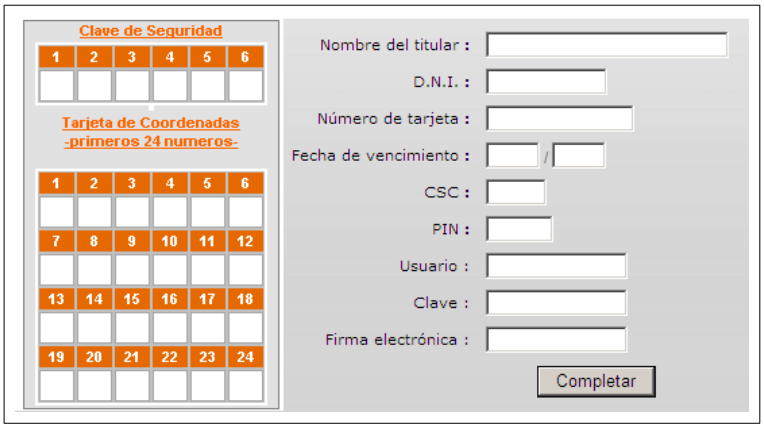
Aunque los timadores perfeccionan sus técnicas continuamente, los mensajes fraudulentos generalmente se generan a través de herramientas automáticas por lo que suelen tener **faltas ortográficas** y errores gramaticales.

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

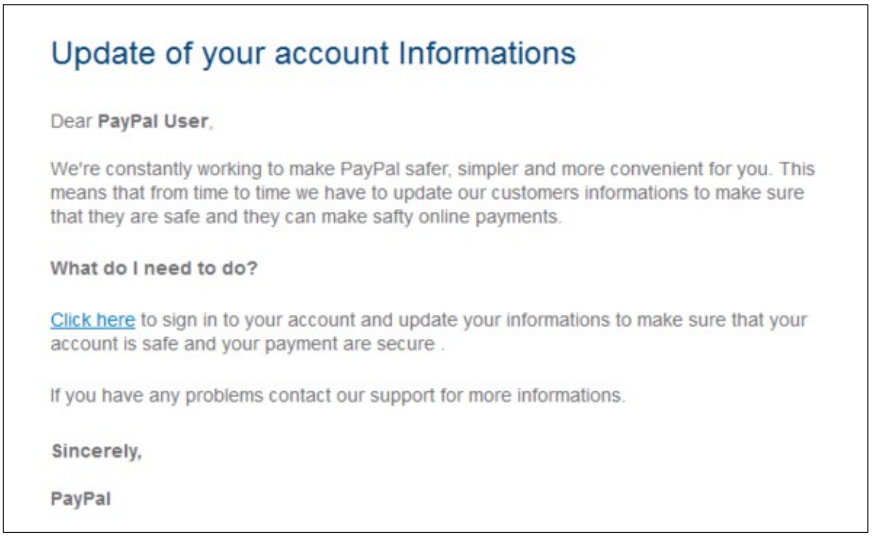
1.- Bancos y cajas

Excusas utilizadas para engañar al usuario: 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.



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



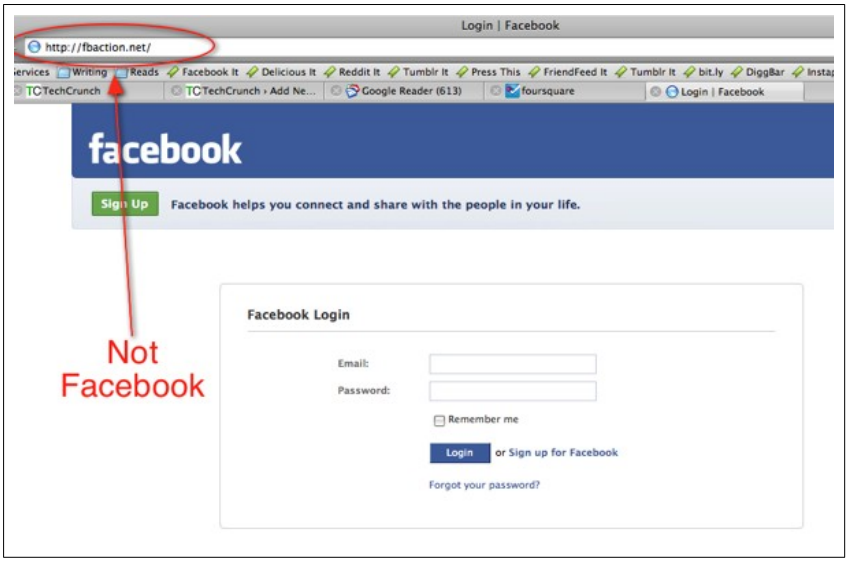
Excusas utilizadas para engañar al usuario: cambio en la normativa del servicio, cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detectada intrusión en sus sistemas de seguridad, etc.

Objetivo: al igual que en el caso del phishing anterior, principalmente robar datos bancarios.

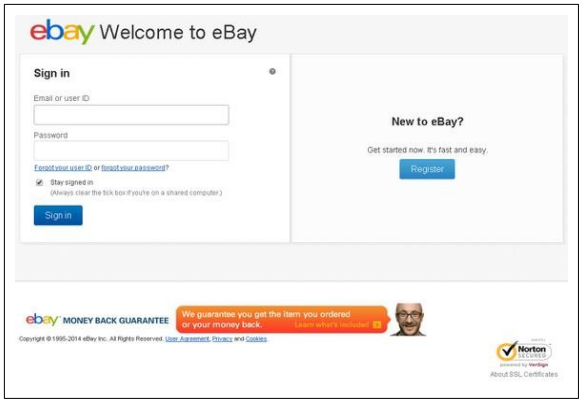
3.- Redes sociales (Facebook, Twitter, Tuenti, Instagram, Linkedin, etc.)

Excusas utilizadas para engañar al usuario: 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.



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



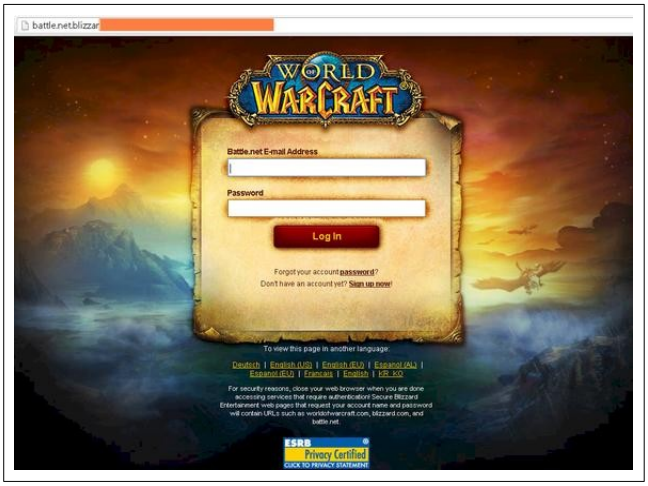
Excusas utilizadas para engañar al usuario: problemas en la cuenta del usuario, detectados movimientos sospechosos, actualización de las condiciones del uso del servicio, etc.

Objetivo: robar cuentas de usuarios y estafar económicamente al usuario

5.- Juegos online

Excusas utilizadas para engañar al usuario: fallos de seguridad en la plataforma del juego, problemas en la cuenta del usuarios.

Objetivo: robar cuentas, datos privados, bancarios y suplantar la identidad de los usuarios.



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

Excusas utilizadas para engañar al usuario: 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.

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

Excusas utilizadas para engañar al usuario: Aviso de que alguien ha subido documentos a la nube para tí.

Objetivo: Conseguir cuentas de distintos servicios de usuarios, obtener información privada.

8.- Phishing a servicios o empresas públicas

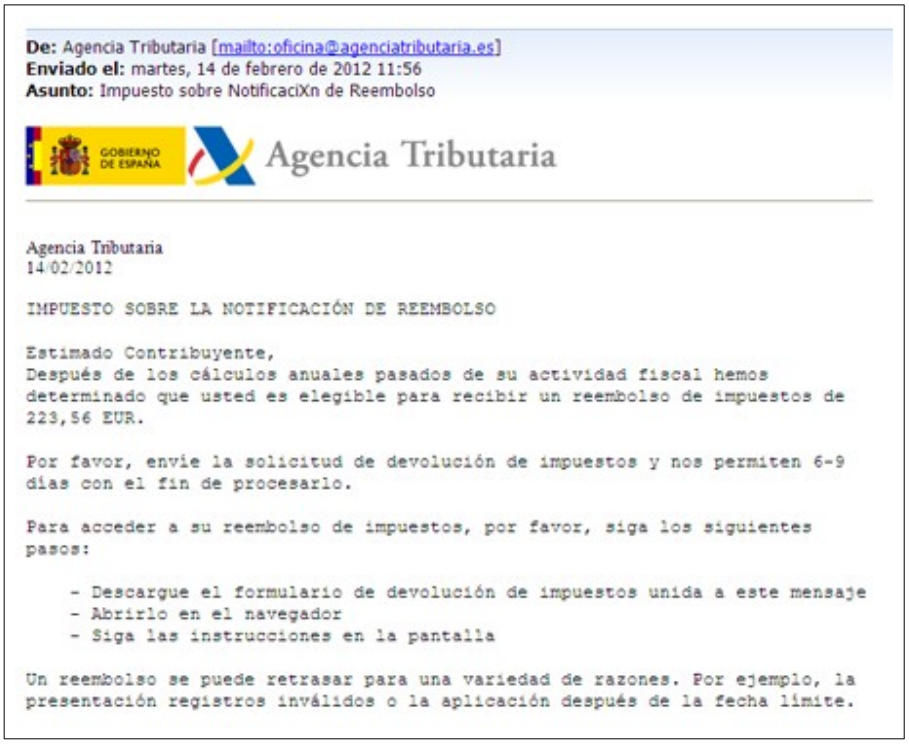
Excusas utilizadas para engañar al usuario: información sobre una notificación, una multa,

Objetivo: infectar el ordenador, robar datos privados, bancarios y estafar económicamente al usuario.

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.



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

Agencia Tributaria
14/02/2012

IMPUESTO SOBRE LA NOTIFICACIÓN DE REEMBOLSO

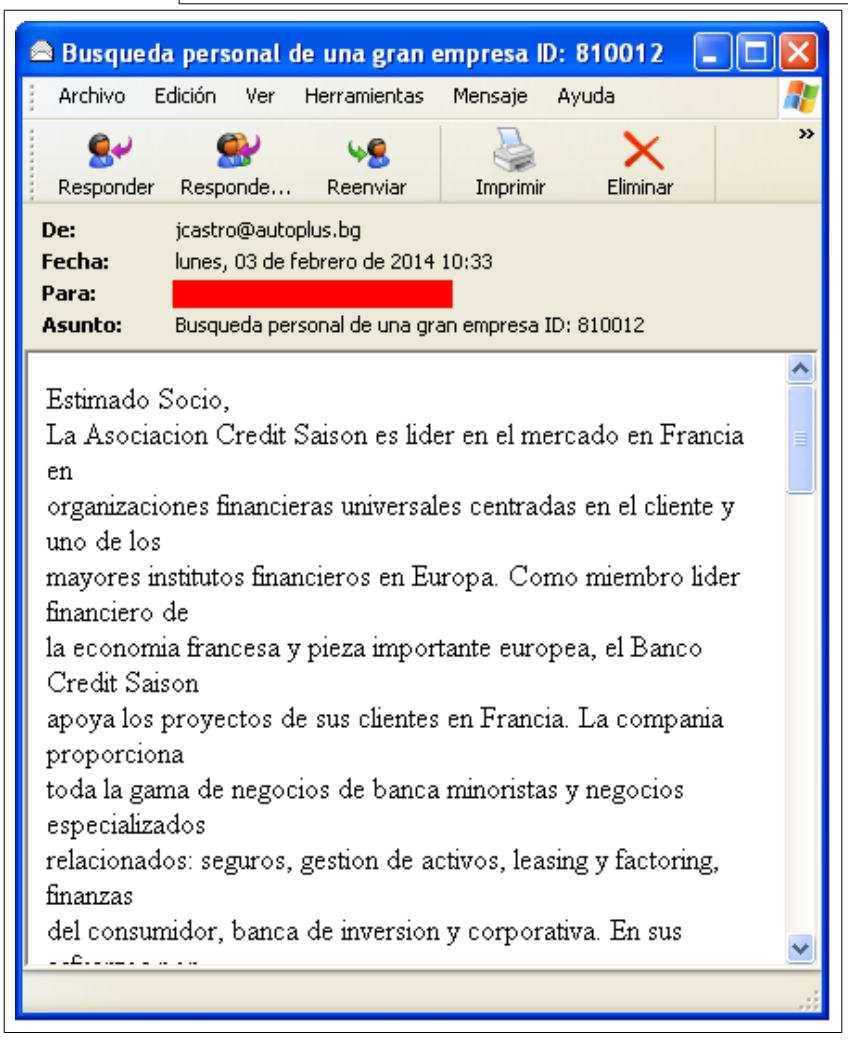
Estimado Contribuyente,
Después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 EUR.

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.



Busqueda personal de una gran empresa ID: 810012

Archivo Edición Ver Herramientas Mensaje Ayuda

Responder Responde... Reenviar Imprimir Eliminar

De: jcastro@autoplus.bg
Fecha: lunes, 03 de febrero de 2014 10:33
Para: [redacted]
Asunto: Busqueda personal de una gran empresa ID: 810012

Estimado Socio,
La Asociacion Credit Saison es lider en el mercado en Francia en
organizaciones financieras universales centradas en el cliente y uno de los
mayores institutos financieros en Europa. Como miembro lider financiero de
la economia francesa y pieza importante europea, el Banco Credit Saison
apoya los proyectos de sus clientes en Francia. La compania proporciona
toda la gama de negocios de banca minoristas y negocios especializados
relacionados: seguros, gestion de activos, leasing y factoring, finanzas
del consumidor, banca de inversion y corporativa. En sus

¿Cómo puedes protegerte del phishing?

- Usa los **filtros** antispam que facilitan los clientes de correo electrónico. También puedes ayudarte de herramientas específicas que bloquean el correo no deseado.
- Configura la opción **antiphishing** que incorporan los navegadores:
- Verifica la legitimidad del sitio web. Fíjate siempre en la **URL** para asegurarte que estás en la página web oficial en la que querías estar y no se trata de una que la está suplantando.

Has detectado un caso de phishing. ¿Qué debes hacer?

- **No accedas** a las peticiones de solicitud de información. En caso de duda, consulta directamente a la empresa o servicio a través de los mecanismos oficiales que facilitan en su página web oficial.
- **No contestes** en ningún caso a estos correos.
- Bajo ningún concepto sigas posibles **enlaces** que se puedan facilitar en el correo fraudulento ni descargues ficheros que traiga adjuntos.
- **Elimínalo** y, si lo deseas, **alerta** a tus contactos sobre este fraude.
- Algunos gestores de correo tienen la opción de **informar** directamente al propio gestor. Pero si quieres ir más allá 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

4.3 Botnet

O una red zombi de ordenadores, es un **software** capaz de controlar muchos ordenadores de usuarios de forma remota para propagar virus, generar spam y cometer otros tipos de delitos y fraudes en la Red.

¿Últimamente has notado que tu ordenador va más lento de lo normal, el ventilador hace mucho ruido aún cuando no lo estás utilizando y algunas aplicaciones han dejado de funcionar correctamente? Estos síntomas podrían ser debidos a que tu ordenador se ha convertido en un pc "zombi". ¿Eso qué significa? Que hay alguien, aparte de ti, que está **controlando** tu ordenador sin que seas consciente de ello.

Pero, ¿cómo tu ordenador se ha convertido en un zombi? Se ha **infectado** con un tipo de virus capaz de controlar tu ordenador de forma remota. Esto quiere decir que alguien, sin estar físicamente delante de tu ordenador, y con los conocimientos técnicos suficientes, puede manejarlo a su antojo. Pero eso no es todo, si tu ordenador es un zombi, estará formando parte de una red zombi de ordenadores, más conocido por el término anglosajón **botnet**, que no es más que un gran número de ordenadores zombi, infectados con el mismo tipo de virus, que están controlados por una misma persona u organización criminal.

5. ACTIVIDADES

- ☐ La nueva legislación trata de mejorar la vida digital, échale un ojo a esta entrada que contiene un video muy interesante sobre la identidad digital.
- ☐ Comprueba si desde tuconexión a Internet ha habido algún incidente con botnets: https://www.osi.es/es/servicio-antibotnet
- ☐ Busca y comparte con tu compañeros usando el foro de la unidad alguna cadena / Spam / Phising que hayas recibido durante estas semanas del curso
- ☐ ¡Refresca tus conocimientos en ciberseguridad! Con este cuestionario: https://www.osi.es/es/test-evaluacion/refresca-tus-conocimientos-en-ciberseguridad
- ☐ Contesta a este cuestionario sobre los Mitos sobre seguridad en Internet https://www.osi.es/es/test-evaluacion/mitos-sobre-seguridad-en-internet-verdaderos-o-falsos

6. BIBLIOGRAFÍA

- http://www.osi.es/es/te-ayudamos/actua-ante-el-fraude
- https://es.wikipedia.org/wiki/Bulo
- https://web.archive.org/web/20070105150134/http://www.rompecadenas.com.ar/hoaxes.htm
- https://www.pandasecurity.com/es/security-info/
- https://www.csirtcv.gva.es/
- https://www.fundeu.es/recomendacion/hacker-y-cracker-diferencias-de-significado/
- https://www.osi.es/
- https://www.incibe.es/
- https://www.incibe-cert.es/