Guardia Civil

“Nuestros mayores ante las nuevas tecnologías”

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

UOPJ CUENCA
22 de noviembre de 2023

CIBERDELINCUENCIA

En los últimos años el crecimiento de los ciberdelitos ha sido exponencial y los ataques son cada vez más estructurados y sofisticados. Y es que cada día consumimos más servicios y productos digitales, lo que inevitablemente hace que aumente nuestra exposición a los ciberdelitos y que estos sean más rentables

Así es que la delincuencia general se está trasladando cada vez en mayor medida al mundo digital

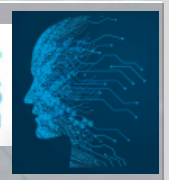
espionaje, sabotaje, terrorismo, ***delito, crimen e incluso guerra***

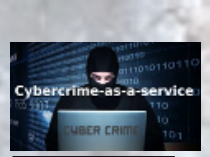
con el denominador común del prefijo
"Ciber-"
diversificando fines, compartiendo tecnologías de ataque y centrando sus objetivos en Internet.

CIBERDELINCUENCIA

Guardia Civil

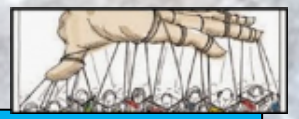
CRIPTOFRAUDES 2020





eCRIME 2016

CaaS 2016



PHISHING 2002

2004 INJURIAS CALUMNIAS AMENAZAS

DESINFORMACIÓN 2014

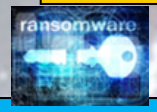
PIRATERÍA

2004 ACOSO INFANTIL GROMING

ESTAFAS COMERCIO ELECTRÓNICO

PORNOGRAFIA INFANTIL

SUPLANTACIONES DE IDENTIDAD 2014



DAÑOS VIRUS TROYANOS

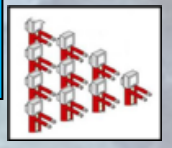
TRÁFICOS Y SERVICIOS ILÍCITOS 2004

RANSOMWARE 2014

CIBERTERRORISMO 2014

HACKTIVISMO 2008

MALWARE BOTNETS 2004



ESPIONAJE POLÍTICO 2014

EXFILTRACIÓN LEAKs 2008

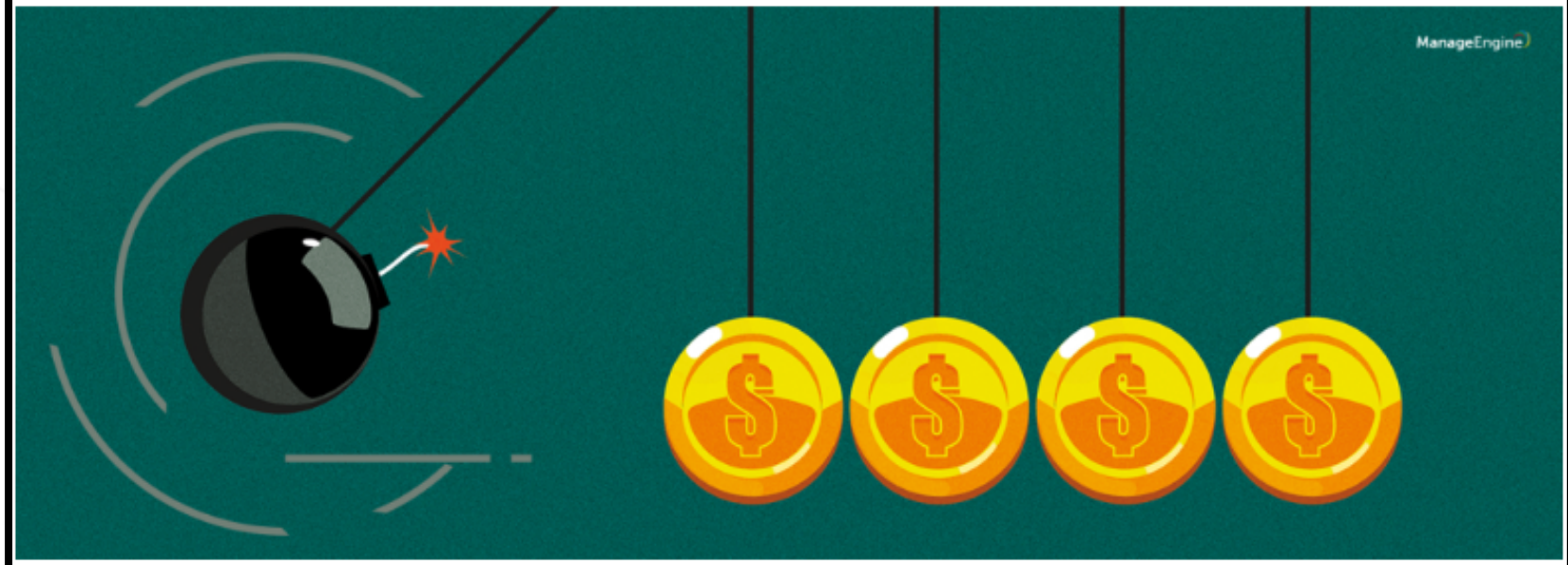
2010 ATP,S ESPIONAJE INDUSTRIAL

CIBERGUERRA 2007

Guardia Civil

La ciberdelincuencia y su impacto en la economía

: 4/7/2022



Para las organizaciones de todo el mundo, la idea errónea de que están protegidas o de que están a salvo de la ciberdelincuencia es lo que conduce a las vulnerabilidades y finalmente, a las violaciones de ciberseguridad.

Según el informe del FBI sobre la delincuencia en Internet en 2021, se registraron 847.000 denuncias y se contabilizaron más de **$6.900 millones de dólares** en pérdidas debido a la ciberdelincuencia en todo el mundo.

¿QUÉ SON LAS ESTAFAS ONLINE?

- Las Estafas en línea son intentos de engañar y robar información personal o financiera a través de internet.
- Los estafadores utilizan tácticas DE INGENIERÍA SOCIAL como correos electrónicos falsos, sitios web fraudulentos o llamadas telefónicas engañosas para llevar a cabo estas estafas.

Ingeniería social

Una de las técnicas por las que un atacante puede obtener información confidencial o nuestras claves de acceso se basa en conseguir engañarnos para hacernos creer que debemos facilitar esa información.

A este comportamiento se le conoce como *ingeniería social*. Algún ejemplo de ello son los correos o llamadas de teléfono que, aparentando ser de nuestro banco, argumentan por cualquier motivo técnico que debemos facilitar nuestras credenciales de acceso.

TIPOS ESTAFAS ONLINE

- PHISHING
- SMISHING
- ESTAFA ROMANCE
- ESTAFA SERVICIO TÉCNICO
- BIZUM INVERSO
- FALSAS INVERSIONES

PHISHING

- El phising es un intento de engañar a las personas para que revelen información confidencial (contraseñas, números tarjetas crédito o datos bancarios). HABITUALMENTE POR MAIL
- Los estafadores envían correos electrónicos o SMS fraudulentos o crean sitios web falsos que se asemejan a los de instituciones legítimas, como bancos o empresas reconocidas
- Objetivo principal: víctimas hagan clic en enlaces maliciosos o proporcionen datos personales o financieros
- Importante tener cuidado al abrir correos electrónicos sospechosos y evitar proporcionar información personal

PHISHING

Guardia Civil

Policía Nacional Siguiendo
@policia

Hoy circula este #phishing. RECUERDA: tu banco nunca te pedirá datos a través de correo electrónico

Banco-Santander-Particulares<instte@xtra.co.nz>

Santander

Estimado cliente,

Lamentamos informarle que hemos bloqueado [redacted] tarjeta de crédito.
Este procedimiento de seguridad [redacted] tarjeta de crédito.

Para que podamos [redacted] seguro, se requiere la verificación de su tarjeta de crédito.
Inicie la confir[redacted], no habrá ningún cargo por usted.
De lo contrario, [redacted] entrega por correo postal dentro de los 14 días hábiles. Esto está asociado con una tarifa de [redacted] EUR, que luego se dedu[redacted] su cuenta

Continuar con la actualización

Esta carta fue enviada por un sistema automatizado de transmisión de mensajes.
La dirección de difusión no es una dirección de correo electrónico clásica.
Si escribe a esta dirección, su mensaje no se tendrá en cuenta

PHISHING

11:02 - 18 mar. 2018

Gmail by Google

Pedro [redacted] <[redacted]@gmail.com>

Reembolso de impuestos de €396,30
1 mensaje

Agencia Tributaria <[redacted]@gmail.com> 14 de febrero de 2016, 15:38
Cco: inf[redacted]@gmail.com

Gobierno de España — Agencia Tributaria

Estimado contribuyente,
Después de que los últimos cálculos anuales usted es elegible para recibir un reembolso de impuestos de €396,30. Para acceder a su devolución de impuestos click "Enviar solicitud de reembolso"
Enviar solicitud de reembolso

La Agencia Tributaria

PHISHING

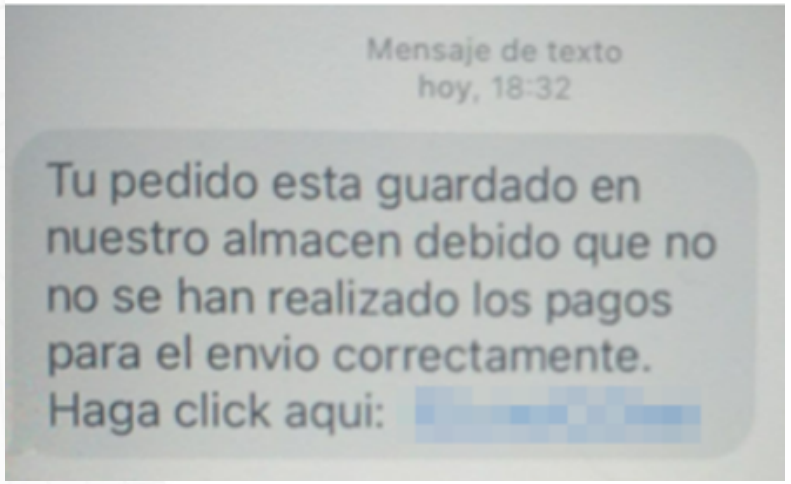
SMISHING

- El smishing es una técnica de ingeniería social que se basa en el envío por parte de los cibercriminales de un mensaje al dispositivo móvil de la víctima simulando ser una empresa determinada o incluso un organismo oficial, junto con un link.
- Al acceder al link, víctima da acceso a su tarjeta SIM y, por tanto a realizar un duplicado; con lo que toda la información que nuestros teléfonos poseen.
- SMS entidades bancarias, CORREOS, servicios paquetería, etc.

SMISHING


14:00
4G
Mensaje de texto
domingo, 11:17
CORREOS: Tu envio esta en camino: https://correos-cdn.com/
Mensaje de texto


martes, 2 de marzo de 2021
Hola Capitn[redacted],
Tiene (1) Paquete de Media Markt!
Ref: UPS-39-03-1233-M
Ultima oportunidad para recogerlo >> https://84blog.xyz /pkg/[redacted]


Mensaje de texto
hoy, 18:32
Tu pedido esta guardado en nuestro almacen debido que no no se han realizado los pagos para el envio correctamente.
Haga click aqui:

ESTAFAS ROMANCE

- Se basan en la construcción de relaciones emocionales con el objetivo de explotar a las personas
- Se hacen pasar por intereses amorosos en línea, ganando la confianza de sus víctimas a través de mensajes y llamadas frecuentes
- Una vez establecido el vínculo, solicitan dinero o información personal
- Presta atención a señales de advertencia como la rapidez con la que se enamoran o la solicitud constante de dinero sin razón clara

ESTAFAS SOPORTE TÉCNICO

- Se hacen pasar por técnicos de soporte de compañías legítimas, como proveedores de servicios de Internet o empresas de software
- Llaman a las personas o muestran anuncios con mensajes de advertencia falsos, afirmaciones de problemas de seguridad o problemas técnicos inexistentes
- Buscan obtener acceso remoto a los dispositivos
- Las compañías legítimas no llamarán de forma inesperada ni solicitarán información confidencial por teléfono o correo electrónico

BIZUM INVERSO

- Primer contacto con plataforma de compraventa de segunda mano para comprar o vender un producto y rápidamente dicen de pasar a una plataforma de mensajería instantánea (Whatsapp…) para eludir los sistemas de pago seguro.
- Dicen realizarnos un pago por Bizum para cubrir gastos envío
- Recibimos un mensaje Bizum en el que escriben “Fulanito le envía 500€ para gastos de envío”; cuando en realidad han utilizado la función de “SOLICITAR” en lugar de la de “ENVIAR”.
- No nos fijamos al estar cegados por la recepción del dinero. Aceptamos y enviamos involuntariamente dicha cantidad

BIZUM INVERSO

Guardia Civil

← Volver al blog

bizum

5. Si recibes una transferencia de dinero o un Bizum, el importe aparecerá automáticamente en tu cuenta bancaria y recibirás una notificación de tu entidad para informarte.

No será necesario que realices ninguna otra gestión ni validación por tu parte.

6. En el caso de recibir una solicitud de envío de dinero a través de Bizum, lee atentamente el SMS y/o la notificación recibidos.

Comprueba que el importe y el nombre del destinatario son correctos. Para aceptar la solicitud de envío de dinero es necesario que accedas a tu aplicación bancaria e introducir un segundo factor de validación. Rechaza la solicitud si no identificas la petición de envío de dinero. Nunca aceptes solicitudes de fuentes desconocidas, compañías con las que no tengas relación y/o Administraciones Públicas u organismos oficiales.

FALSOS INVERSORES

- OJO CRIPTOMONEDAS. Algunas ofertas de inversión pueden ser estafas diseñadas para engañar y robar dinero. Investiga antes de invertir y elige proyectos confiables.
- No te dejes llevar por la información exagerada sobre el rápido aumento de precios de una criptomoneda. Algunos estafadores promueven una moneda para venderla rápidamente y dejar a los inversores con pérdidas.
- Cuidado con promesas de altos rendimientos garantizados. Algunos estafadores utilizan el dinero de nuevos inversores para pagar a los anteriores, hasta que el esquema colapsa y se pierde todo

FALSOS INVERSORES

Noticias de Tudela

Estafan 32.000 euros a una vecina de Tudela a través de una plataforma de inversiones no regulada

UNA VECINA DE TUDELA HA PRESENTADO UNA DENUNCIA PENAL POR UN SUPUESTO FRAUDE CONTRA HELLO TECHNOLOGY

JESÚS MORALES | PAMPLONA | 17.02.2022 | 19:09

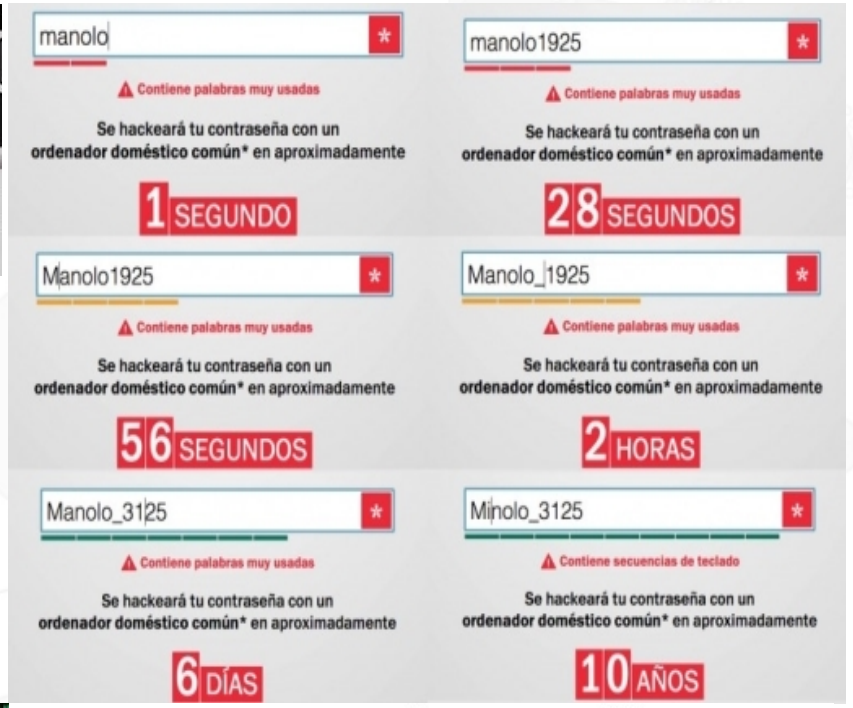
¿Cómo protegerse ante Cibercriminales?

1. Utilizar contraseñas robustas (mayúsculas, minúsculas, números, símbolos)
2. No usar contraseñas recicladas (la misma contraseña para distintos accesos)
3. Utilizar preguntas de seguridad complejas
4. Si es posible, aplicar doble factor de autenticación
5. Subir a nube solo información cifrada
6. Tener conciencia de la información que se está exponiendo a Internet
7. Revisar quién está detrás de un perfil a través de confirmación de imágenes
8. Desactivar permisos de acceso no deseados de aplicaciones en dispositivos móviles (uso de cámara, ubicación, contactos, micrófono, etc.).

Guardia Civil

NO

SI



Largo	Minúscula	Agrega Mayúscula	Números y símbolos
6 caracteres	10 minutos	10 horas	18 días
7 caracteres	4 horas	23 días	4 años
8 caracteres	4 días	3 años	463 años
9 caracteres	4 meses	178 años	44.530 años

Guardia Civil

MUCHAS GRACIAS
POR SU ATENCIÓN

Art. 6 Cartilla del Guardia Civil:

"…Procurará ser siempre un pronóstico feliz para el afligido…"

Cap. Aarón Navas Aragüete
Jefe UOPJ Cuenca
anavasa@guardiacivil.es
649 95 11 69

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR