OFICINA Acelera pyme

CIBERSEGURIDAD FÁCIL: CÓMO DEFENDER A TU EMPRESA DE LAS AMENAZAS INFORMÁTICAS

7 DE FEBRERO DEL 2024

caixa popular

Financiado por la Unión Europea

GOBIERNO DE ESPAÑA · MINISTERIO DE TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Fondos Europeos

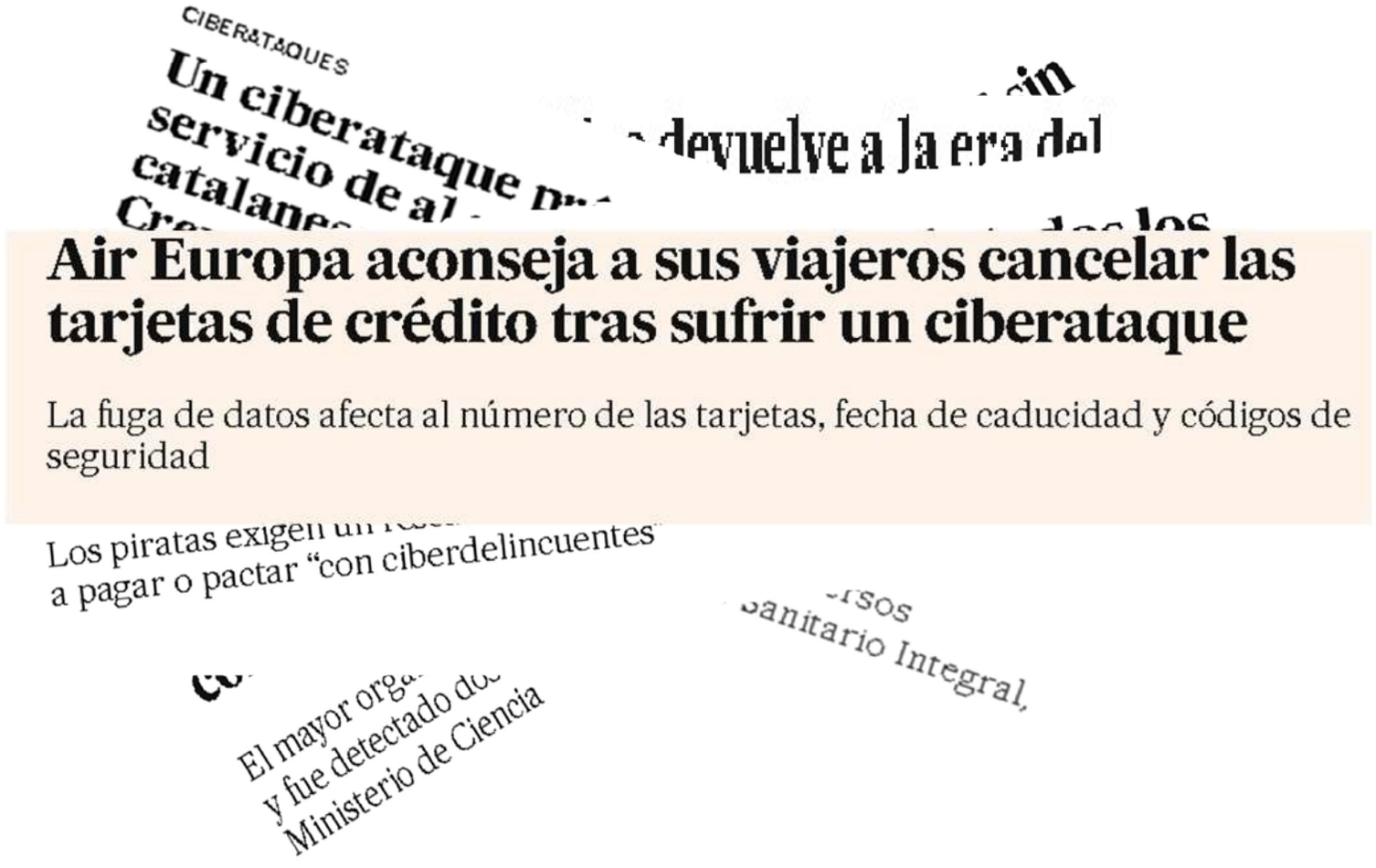
Fondo Europeo de Desarrollo Regional

"Europa se siente"

CiberSeguridad , ¿moda o realidad?

- Una de cada dos empresas españolas sufrió ciberataques en 2021.
- De media, 40.000 ciberataques al día en 2021, lo que implica un 125 % mas que el año anterior.
- En 2022, España se posiciona como el tercer país que más ciberataques sufre, solo por detrás de Estados Unidos y Alemania.
- 2022 se despidió con un incremento del 28% en ciberataques

El auge de los ciberataques



CIBERATAQUES

Un ciberataque [illegible] devuelve a la era del servicio de al[illegible]

catalane[illegible]

Air Europa aconseja a sus viajeros cancelar las tarjetas de crédito tras sufrir un ciberataque

La fuga de datos afecta al número de las tarjetas, fecha de caducidad y códigos de seguridad

Los piratas exigen un [illegible] a pagar o pactar "con ciberdelincuentes"

[illegible]rsos

Sanitario Integral,

El mayor orga[illegible]

y fue detectado do[illegible]

Ministerio de Ciencia

Algunas cosas han cambiado:

- El Teletrabajo.
- Una necesidad de las compañías de acelerar la transformación digital.

Porque estos incrementos

A quien van Dirigidos

- Gobierno.
- Sanidad.
- Banca.
- Telecomunicaciones.

Actualmente la tendencia esta cambiando ya que el 70% de los ciberataques están destinados a pequeños y medianos negocios.

- Son la puerta de entrada a las grandes empresas.
- El 99,8 % no se considera un objetivo de los ciberataques.
- Ponen más atención en esas empresas donde han encontrado la posibilidad de atacar.
- Atacantes invierten menos recursos y aunque el botín sea menor el beneficio global mejora.

Porque están en el punto de mira de los hackers

Efectos en pequeños y medianos Negocios

- El coste promedio de un ciberataque tiene un coste de 35.000 Eu.
- El 60 % de los negocios víctimas de un ciberataque desaparece a los 6 Meses.
- Tardan 212 días en detectar un ataque y 75 días en contenerlo.

CIBERSEGURIDAD FÁCIL: CÓMO DEFENDER A TU EMPRESA DE LAS AMENAZAS INFORMÁTICAS

El 55 %
Emai , SMS, WathsApp

El 20 %
Web

El 15 %
Software

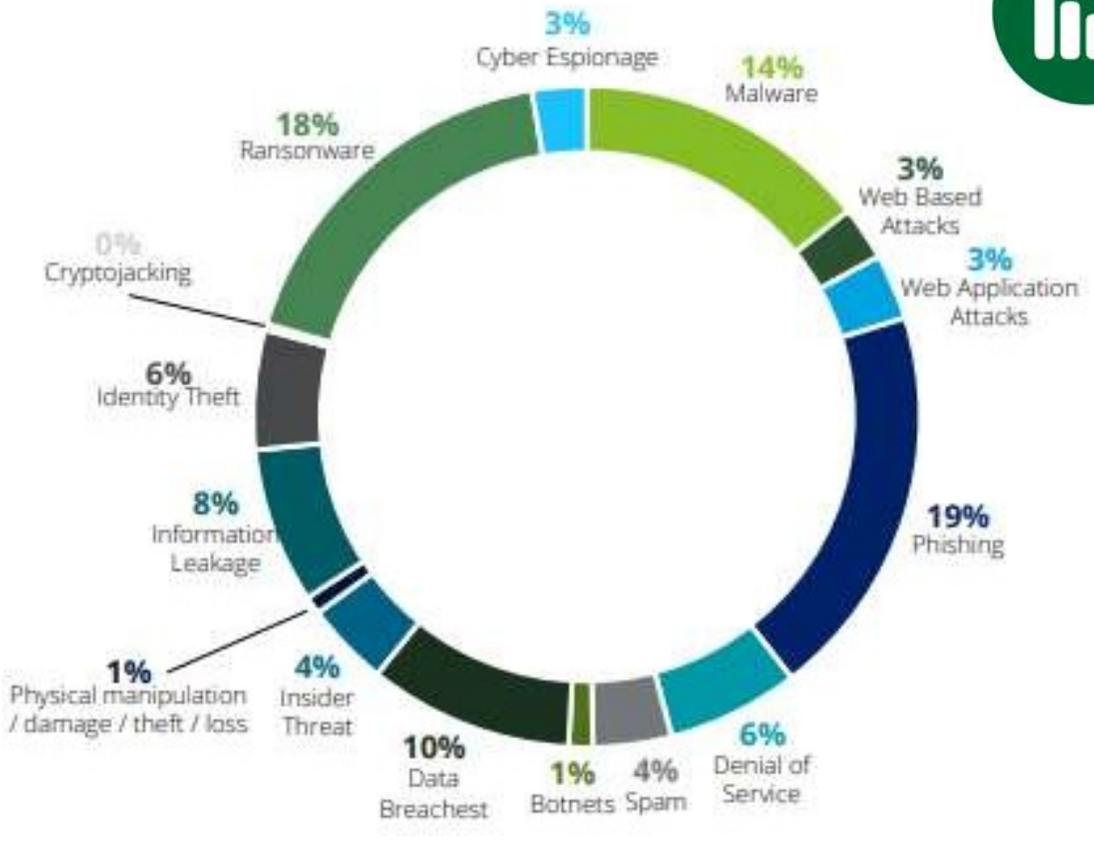
El 10 %
USB / dispositivos

Como llegan las amenazas

La mayoría de amenazas llegan por correo electrónico

Tipos de ataques

- ✓ Phishing 19 %.
- ✓ Ransomware 18%.
- ✓ Malware 14%.
- ✓ Spoofing 6%.



TENDENCIAS: QRISHING

TENDENCIAS: QRISHING

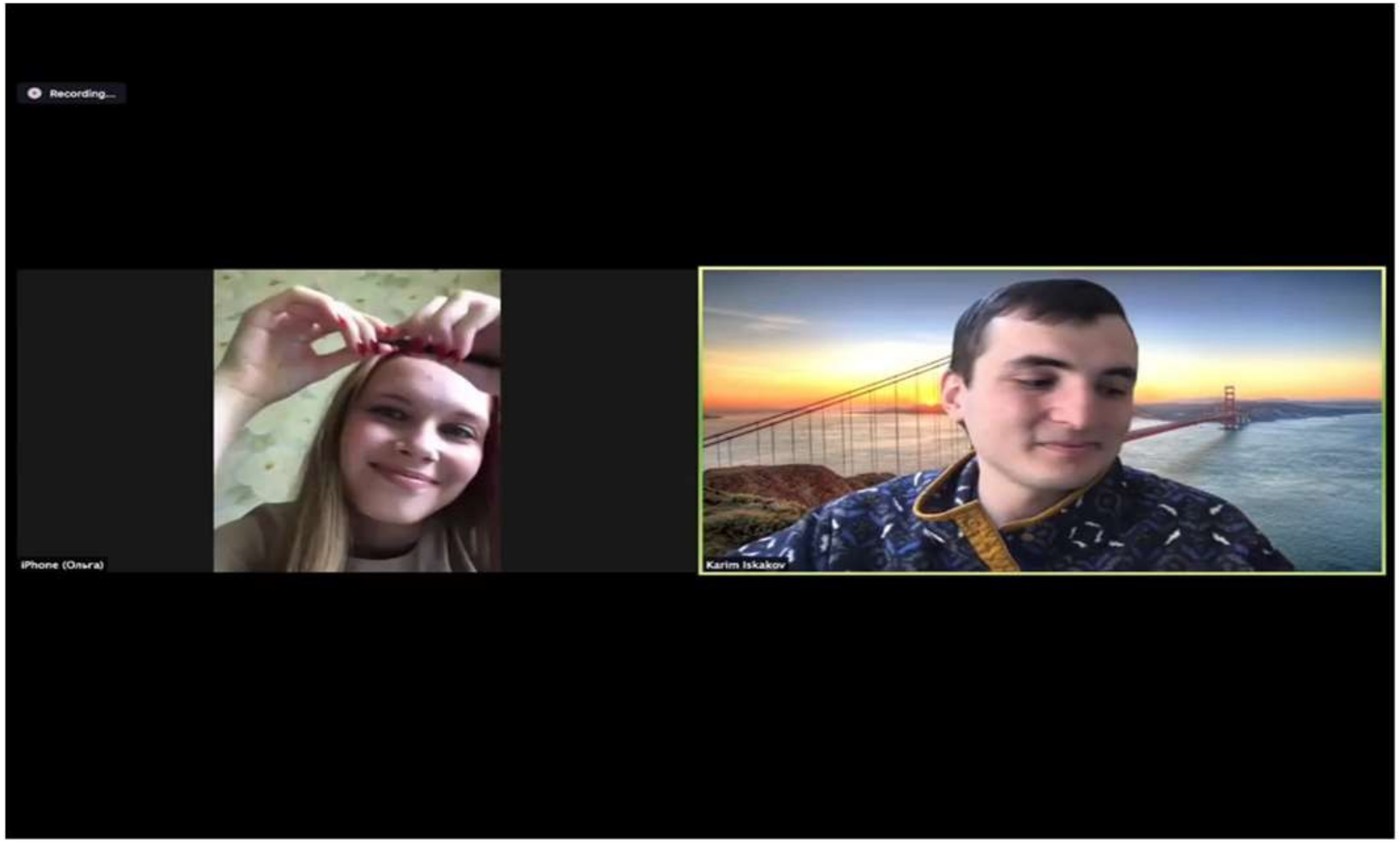
- Multas de Tráfico: Web falsa.
- QR Inverso.
- Pegatinas: Establecimientos y Carteles compra entradas

TENDENCIAS: BIZUM

TENDENCIAS: BIZUM

- BIZUM Inverso: Nos solicitan dinero.
- No se puede anular en envío.
- Entidades Oficiales NO trabajan con BIZUM.
- Bulos: No nos pueden clonar los datos bancarios

TENDENCIAS: IA y METAVERSO



Inversión en Tecnología

Tecnología
Dominio Propio
Correo Corporativo
Antivirus Profesional
Copias de Seguridad fuera de línea(nube)
Cortafuegos
SW con licencia
Validación Usuarios y permisos
NO USB
Multifactor Autentificaciόm

CIBERSEGURIDAD FÁCIL: CÓMO DEFENDER A TU EMPRESA DE LAS AMENAZAS INFORMÁTICAS

caixa popular

OFICINA Acelera pyme
FEMEVAL
red.es
Fondos Europeos
Fondo Europeo de Desarrollo Regional
"Europa se siente"

La desconfianza es la madre de la seguridad.

Inversión en Personas

El 85% de los ataques son consecuencia del error humano.

.

- ✓ Formación y Planes de Concienciación.
- ✓ El Rol del CISO.

CIBERSEGURIDAD FÁCIL: CÓMO DEFENDER A TU EMPRESA DE LAS AMENAZAS INFORMÁTICAS

caixa popular

Por donde empezar: https://www.incibe.es

Cualquier tipo de intento de engañarle para que haga algo que beneficie a los delincuentes.

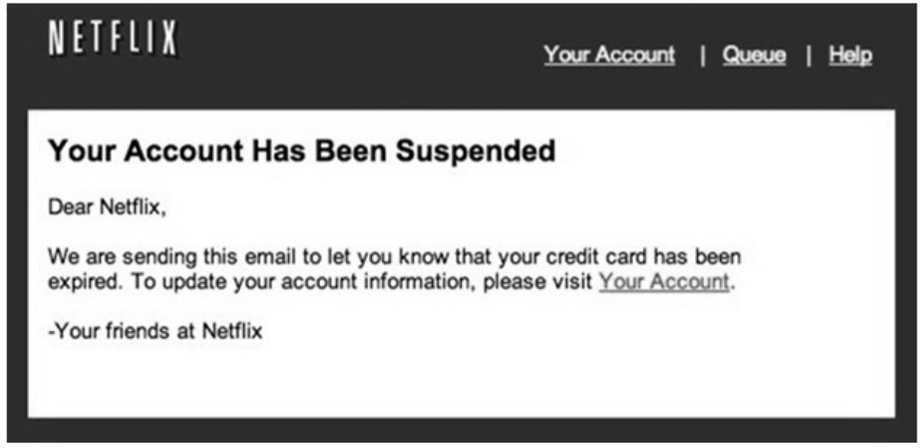
- Abrir un archivo adjunto en un correo electrónico
- Hacer clic en un enlace
- Compartir información confidencial
- Transferir fondos

PHISHING MASIVO

SPEAR PHISHING

¿Qué es el phishing?

- Objetivo: recursos de individuos, como cuentas bancarias, identidad o credenciales de inicio de sesión
- Suele dirigirse a los consumidores
- Impersonal: envíos de correo electrónico en masa
- Se usan o venden credenciales para obtener un beneficio económico



PHISHING MASIVO

Phishing masivo

¿Qué tienen en común estas marcas?

Las 3 marcas más falsificadas en ataques de phishing

Los correos de phishing más efectivos

Asunto Correo Electronico	%Clic
Se te ha asignado una tarea	39%
Paquete Entrega Pendiente	31%
Reunión de la próxima semana	29%
Coche que se ha dejado las luces encendidas	25%
Citacion de Trafico u organismo publico	20%
Hombre sospechoso en edificio	19%
IMPORTANTE - Encuesta anual a los empleados	18%
Revise las Vacaciones	14%

** Porcentaje de mensajes de correo electrónico que se abrieron y en los que el usuario hizo clic en un enlace*

1. Hay algo que no encaja

- ✓ ¿Algo parece raro?
- ✓ ¿Es demasiado bueno para ser verdad?
- ✓ Confíe en su instinto

Los 10 correos de phishing más efectivos

Los 10 correos de phishing más efectivos

Demasiado bueno para ser verdad

Carrefour

BIENVENIDOS A CARREFOUR.

Hola [redacted] !

Hemos escogido a 150 consumidores españoles para participar en una breve encuesta de Carrefour.

Todos los participantes recibirán (1) premio a elegir. Escoge entre tarjetas regalo, electrónica, cupones y muchos más.

Descuento Nasta 90-95%

Haz clic en EMPEZAR para continuar.

EMPEZAR

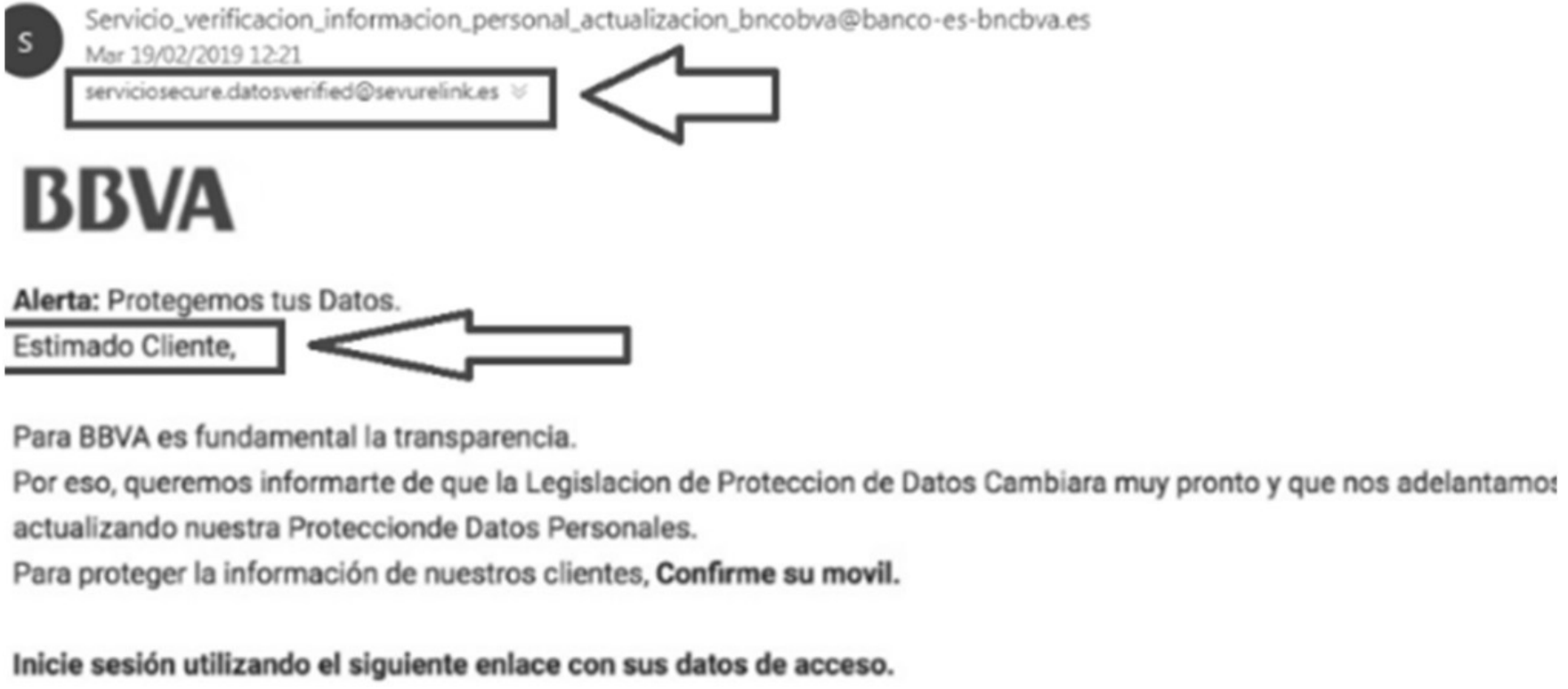
¡Responde lo más rápido posible, los mejores premios serán los primeros!

Los 10 correos de phishing más efectivos

1. Hay algo que no encaja

2. Saludos genéricos

Los 10 correos de phishing más efectivos



S Servicio_verificacion_informacion_personal_actualizacion_bncobva@banco-es-bncbva.es
Mar 19/02/2019 12:21
serviciosecure.datosverified@sevurelink.es

BBVA

Alerta: Protegemos tus Datos.
Estimado Cliente,

Para BBVA es fundamental la transparencia.
Por eso, queremos informarte de que la Legislacion de Proteccion de Datos Cambiara muy pronto y que nos adelantamos
actualizando nuestra Proteccionde Datos Personales.
Para proteger la información de nuestros clientes, **Confirme su movil.**

Inicie sesión utilizando el siguiente enlace con sus datos de acceso.

1. Hay algo que no encaja
2. Saludos genéricos
3. Sitio de aspecto oficial pidiéndole que introduzca datos confidenciales

Los 10 correos de phishing más efectivos

Los 10 correos de phishing más efectivos

Correos españa <[redacted]@bradfordskips.com>

Carta Certificada CD 61278791640

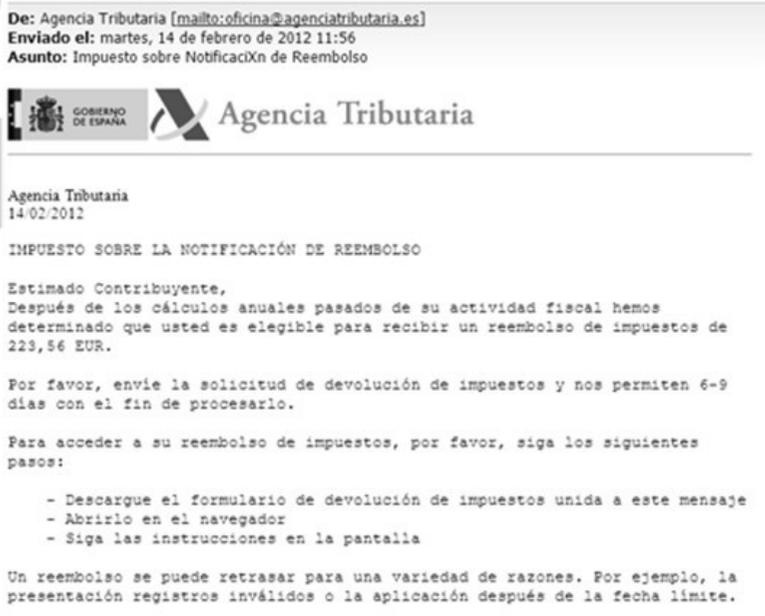
CORREOS

Su paquete ha llegado a **30 de agosto de 2016**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.

CD 61278791640

Descargar información sobre su envío

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de 9,79 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las



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

GOBIERNO DE ESPAÑA 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:

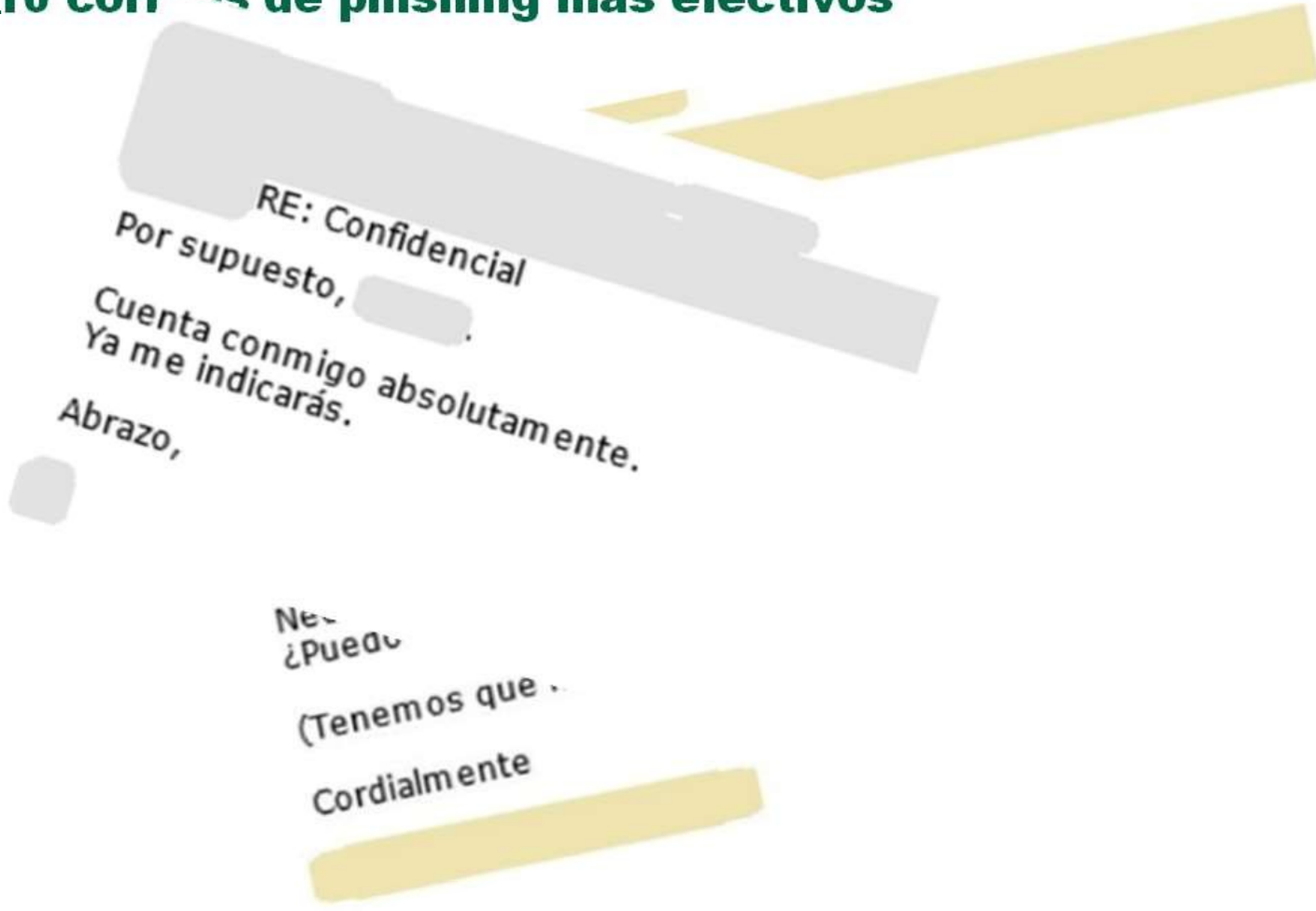
- Descargue el formulario de devolución de impuestos unida a este mensaje
- Abrirlo en el navegador
- Siga las instrucciones en la pantalla

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

Los 10 correos de phishing más efectivos

1. Hay algo que no encaja
2. Saludos genéricos
3. Sitio de aspecto oficial pidiéndole que introduzca datos confidenciales
4. Correo electrónico inesperado; información específicamente para USTED

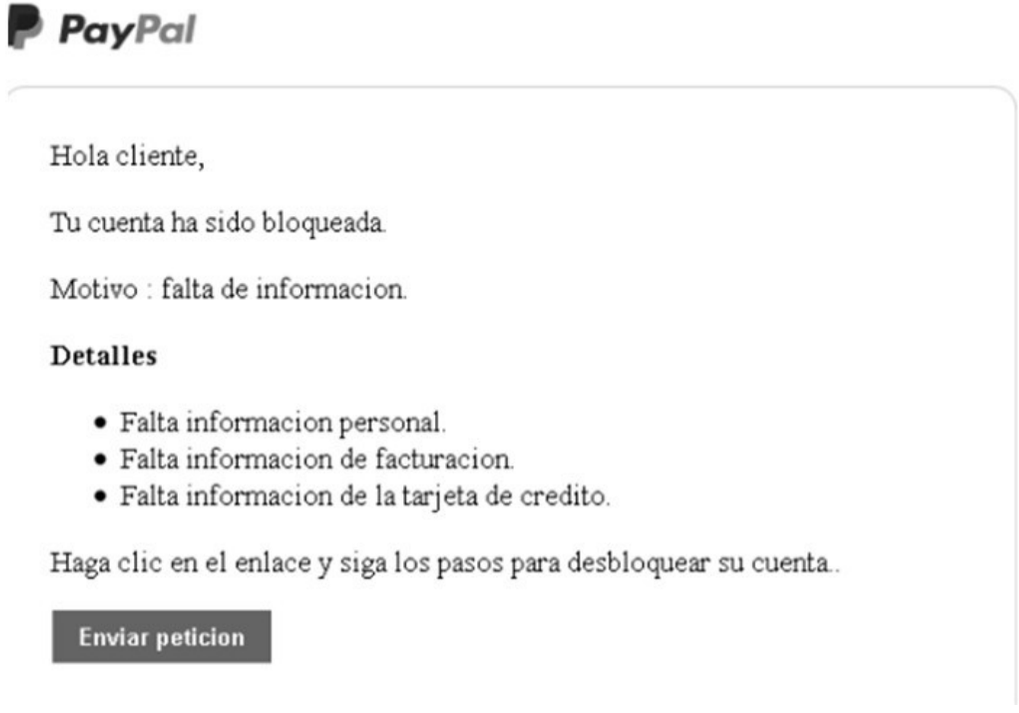
Los 10 correos de phishing más efectivos



Los 10 correos de phishing más efectivos

1. Hay algo que no encaja
2. Saludos genéricos
3. Sitio de aspecto oficial pidiéndole que introduzca datos confidenciales
4. Correo electrónico inesperado; información específicamente para USTED
5. Mensajes alarmantes

Los 10 correos de phishing más efectivos



PayPal

Hola cliente,

Tu cuenta ha sido bloqueada.

Motivo : falta de informacion.

Detalles

- Falta informacion personal.
- Falta informacion de facturacion.
- Falta informacion de la tarjeta de credito.

Haga clic en el enlace y siga los pasos para desbloquear su cuenta..

Enviar peticion

Los 10 correos de phishing más efectivos

1. Hay algo que no encaja
2. Saludos genéricos
3. Sitio de aspecto oficial pidiéndole que introduzca datos confidenciales
4. Correo electrónico inesperado; información específicamente para USTED
5. Mensajes alarmantes
6. Errores gramaticales u ortográficos (o ambos)

Los 10 correos de phishing más efectivos

1. Hay algo que no encaja
2. Saludos genéricos
3. Sitio de aspecto oficial pidiéndole que introduzca datos confidenciales
4. Correo electrónico inesperado; información específicamente para USTED
5. Mensajes alarmantes
6. Errores gramaticales u ortográficos (o ambos)
7. Sensación de urgencia

Los 10 correos de phishing más efectivos

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

Los 10 correos de phishing más efectivos

1. Hay algo que no encaja
2. Saludos genéricos
3. Sitio de aspecto oficial pidiéndole que introduzca datos confidenciales
4. Correo electrónico inesperado; información específicamente para USTED
5. Mensajes alarmantes
6. Errores gramaticales u ortográficos (o ambos)
7. Sensación de urgencia
8. "Ha ganado el primer premio"

Los 10 correos de phishing más efectivos

De: "Loteria Nacional" <k[redacted]a@driv[redacted]n.ne.jp>
A:
Asunto: Notificacion de Premio 915,000.00Euros
Fecha: Fri, 28 Oct

Atencion,

ENHORABUENA
Buscar Adjunto de la notificacion de premio
Por favor, Rellenar este formulario para el proceso del pago y envirlo
Por la agente SARAPHINA SECURITY SERVICES por fax: 0044 208-082-5519

Antonio Williams
(director)

Los 10 correos de phishing más efectivos

1. Hay algo que no encaja
2. Saludos genéricos
3. Sitio de aspecto oficial pidiéndole que introduzca datos confidenciales
4. Correo electrónico inesperado; información específicamente para USTED
5. Mensajes alarmantes
6. Errores gramaticales u ortográficos (o ambos)
7. Sensación de urgencia
8. "Ha ganado el primer premio"
9. "Verifique su cuenta"

Los 10 correos de phishing más efectivos

De Nuevo mensaje [redacted]
Asunto **RuralVia - Caja Rural**
A [redacted]

Hola,

Deseamos informarle de que tiene una nueva actualizacion actualización.

Consulte su correo haciendo clic en el enlace de abajo:

Consulte a la bandeja de entrada

Le damos las gracias por su confianza

Atentamente,

RuralVia - Caja Rural

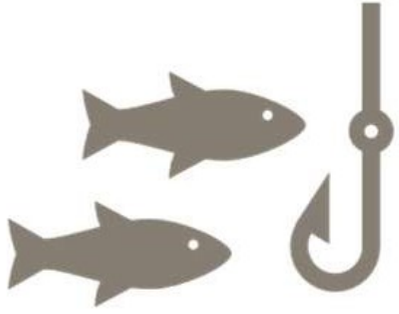
Este correo se le envía automáticamente, no utilice la función "responder al remitente"

Los 10 correos de phishing más efectivos

1. Hay algo que no encaja
2. Saludos genéricos
3. Sitio de aspecto oficial pidiéndole que introduzca datos confidenciales
4. Correo electrónico inesperado; información específicamente para USTED
5. Mensajes alarmantes
6. Errores gramaticales u ortográficos (o ambos)
7. Sensación de urgencia
8. "Ha ganado el primer premio"
9. "Verifique su cuenta"
10. Ciberocupación

www.g00gle.com
frente a
www.google.com

Lista de comprobación



P Promesas

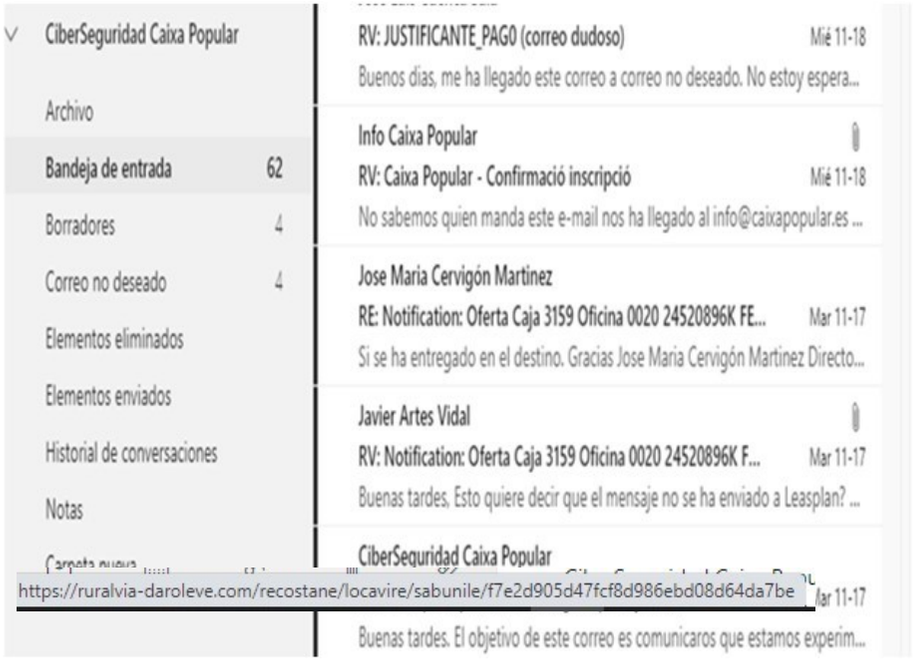
H Hostigamiento

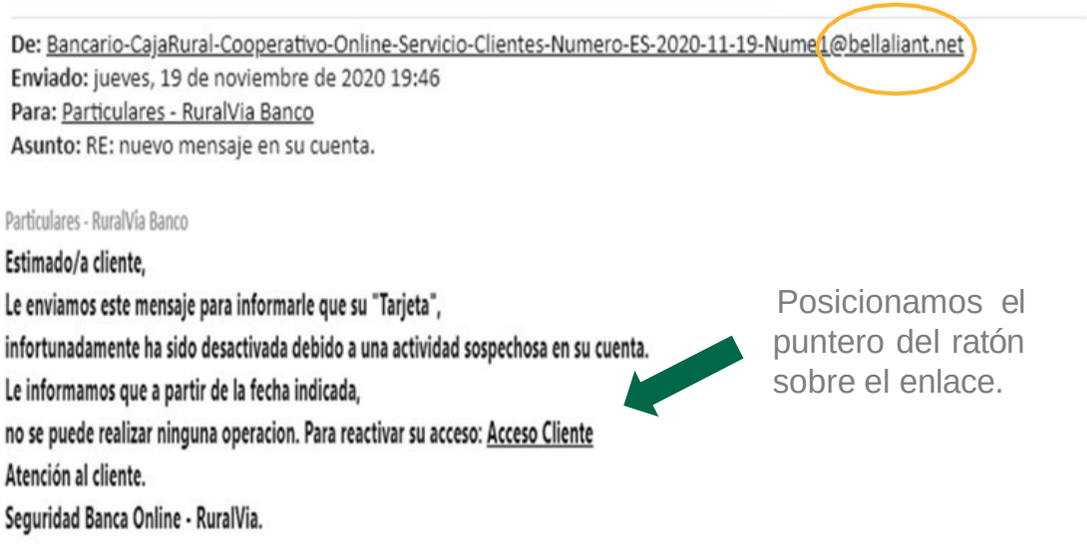
I Impulso

S Sensación de urgencia

H HELIMINAR

Cómo revisar los correos





Posicionamos el puntero del ratón sobre el enlace.

https://ruralvia-daroleve.com/recostane/locavire/sabunile/f7e2d905d47fcf8d986ebd08d64da7be

Casos reales

Suplantación de Identidad

De: asanz@caixapopular.es <kanto@nst-sumisys.co.jp>
Enviado: jueves, 29 de octubre de 2020 18:41
Para: Jose Mayans Mateos <jmayans@caixapopular.es>
Asunto: RE: Hipoteca CLINICA VETERINARIA DOMESTICS SL

"Missatge extern a Caixa Popular" - Teniu precaució abans d'obrir enllaços o fitxers adjunt. Informeu tots els correus electrònics sospitosos a "ciberseguridad@caixapopular.es"

asanz@caixapopular.es

De: asanz@caixapopular.es <kanto@nst-sumisys.co.jp>

Buenas tardes,

adjuntamos Minuta para su confección,
cuya firma está prevista para el próximo miércoles, 4 de diciembre.

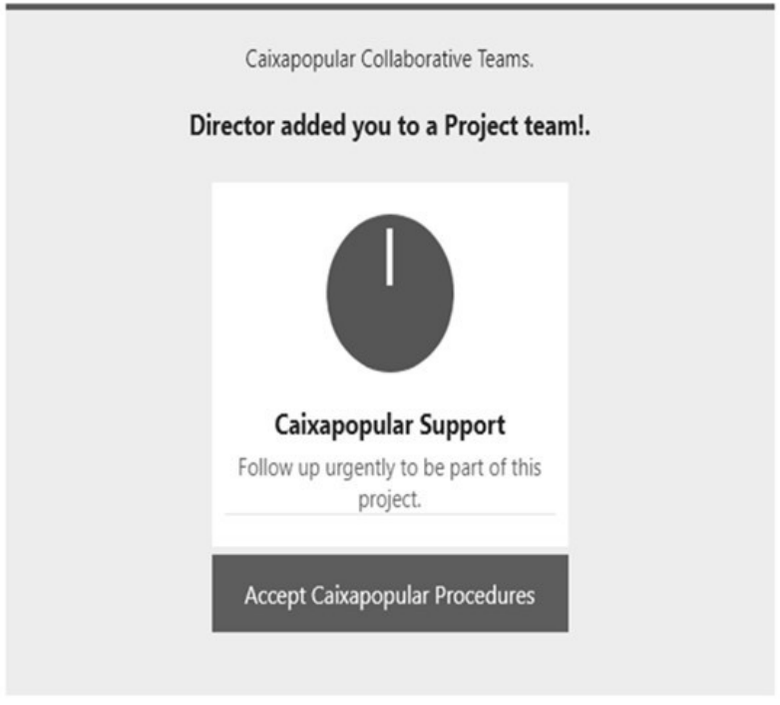
Adjuntamos también la documentación
necesaria para la confección de la misma.

Igualmente, indicarles que, según se
indica en la minuta, **TODAS**
las copias que se emitan de la escritura referente a esta operación, deben expedirse con carácter NO ejecutivo.

En los casos en que
el apoderado de Caixa Popular firme como mandatario verbal, rogamos que
gestionen su ratificación mediante correo notarial, o telemáticamente,
a la notaría de José Vicente Roig Dalmau.

Casos reales

De: Webinar Caixapopular <norepies-caixapopular7dQ6@caixapopular.es>
Enviado: lunes, 28 de septiembre de 2020 11:27
Para: Isabel Montero Lopez <imontero@caixapopular.es>
Asunto: [Webinar project!] You have been added to team



Nos han suplantado en Office 365

DESCONFIAR DE TODOS LOS MENSAJES EN OTROS IDIOMAS

Casos reales

RE: C

De: Atencion al Cliente <ylqfrhxc@cp.amigo7host.net>
Enviado: miércoles, 2 de diciembre de 2020 15:01
Para: Info Caixa Popular <Info@caixapopular.es>
Asunto: CAIXA POPULAR CAIXA RURAL COOP DE CREDITO V Atencion al Cliente

Información de la cuenta

Nombre de la organización: CAIXA POPULAR CAIXA RURAL COOP DE CREDITO V, AVENIDA AL VEDAT, 123 - 125, 46900 Torrent - Spain

Dominio: info@caixapopular.es

Dominio: info@caixapopular.es

Declaración de privacidad
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Microsoft

Casos reales

Microsoft

Security Authentication| Scan Me

De: telnet.info6457@nrep.budpalmer.com <telnet.info6457@nrep.budpalmer.com> en nombre de Online Caixapopular Notification <telnet.info6457@nrep.budpalmer.com>

Enviado: martes, 23 de mayo de 2023 19:28

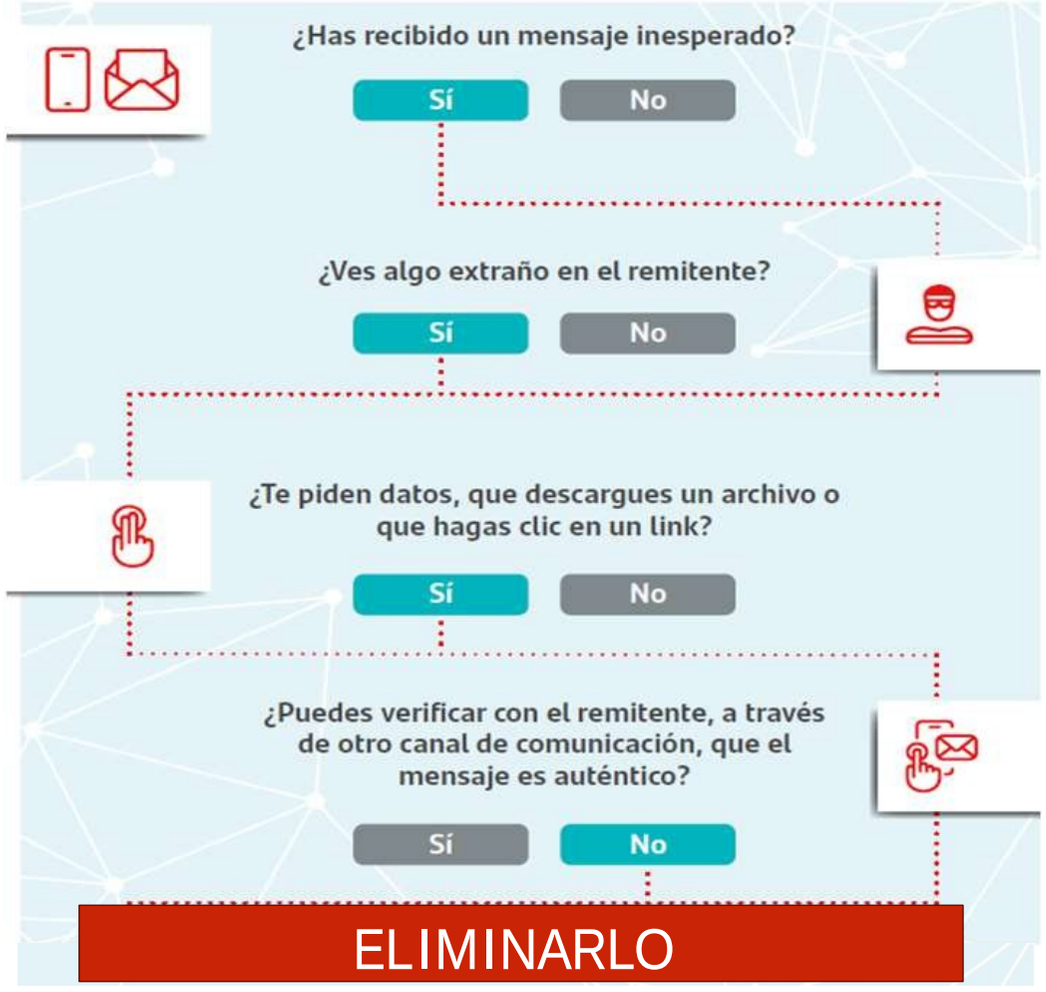
Para: Alicia Soler Belenguer <asoler@caixapopular.es>

Asunto: Notification -Mail- Delivery Online :Authentication-Mail:

Asoler, you are being held responsible to review security update as of **23/05/2023**. **Quickly scan above QR Code with your phone camera.**

Review security requirements within **2 days of the received date** by going to Account manager in the Security Center.

Detección Objetiva PHISING



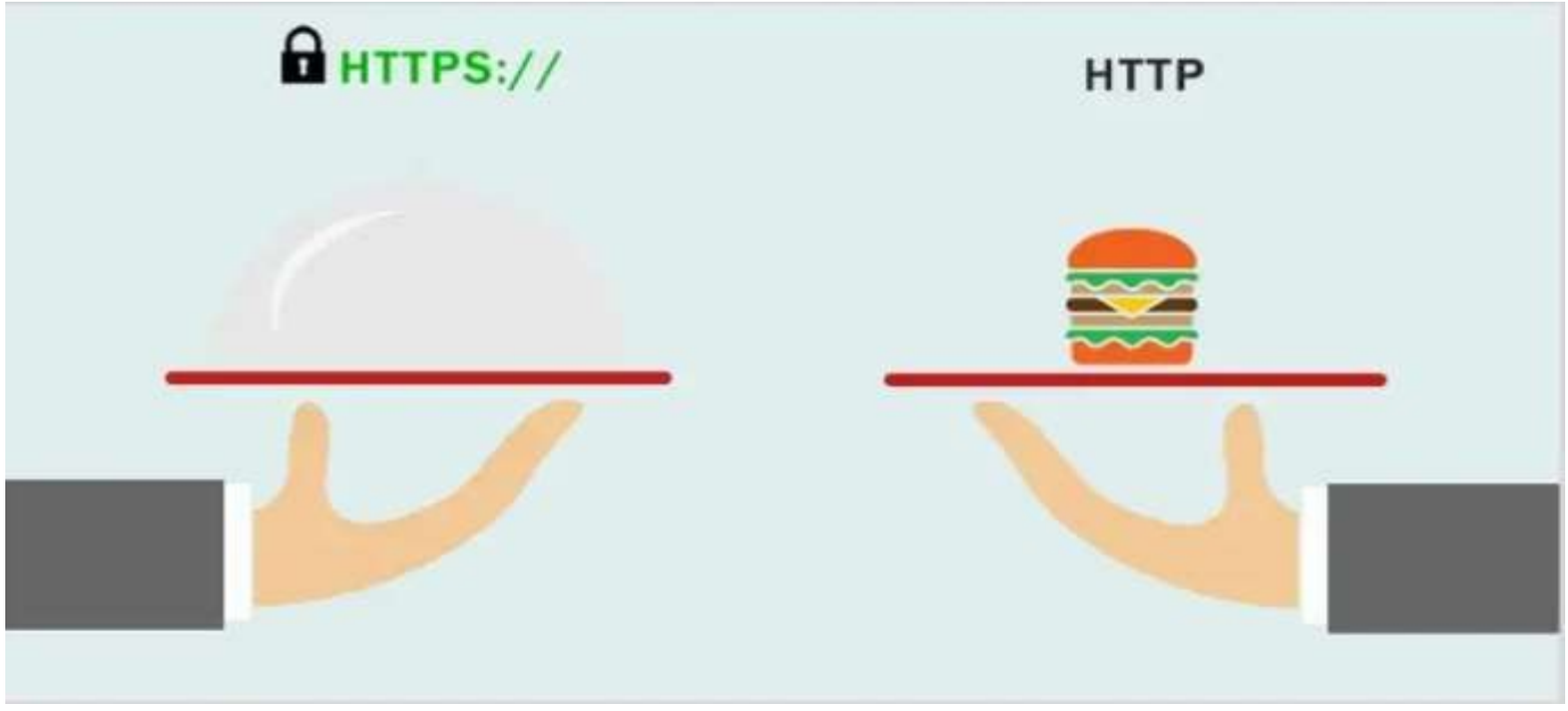
Normalmente nos conectamos a la paginas web con HTTP pero hay que estar atentos a los detalles nos falta la S de SEGURO.

Si los datos son transferidos mediante HTTP, estos viajan en claro y son accesibles para cualquiera que intercepte la comunicación. En cambio, el protocolo HTTPS usa una **conexión segura** mediante un cifrado SSL y por tanto los datos viajan de un modo seguro de un lugar a otro.

El certificado SSL garantiza que la comunicación no se podrá leer ni manipular y que la información personal no caerá en las manos equivocadas.

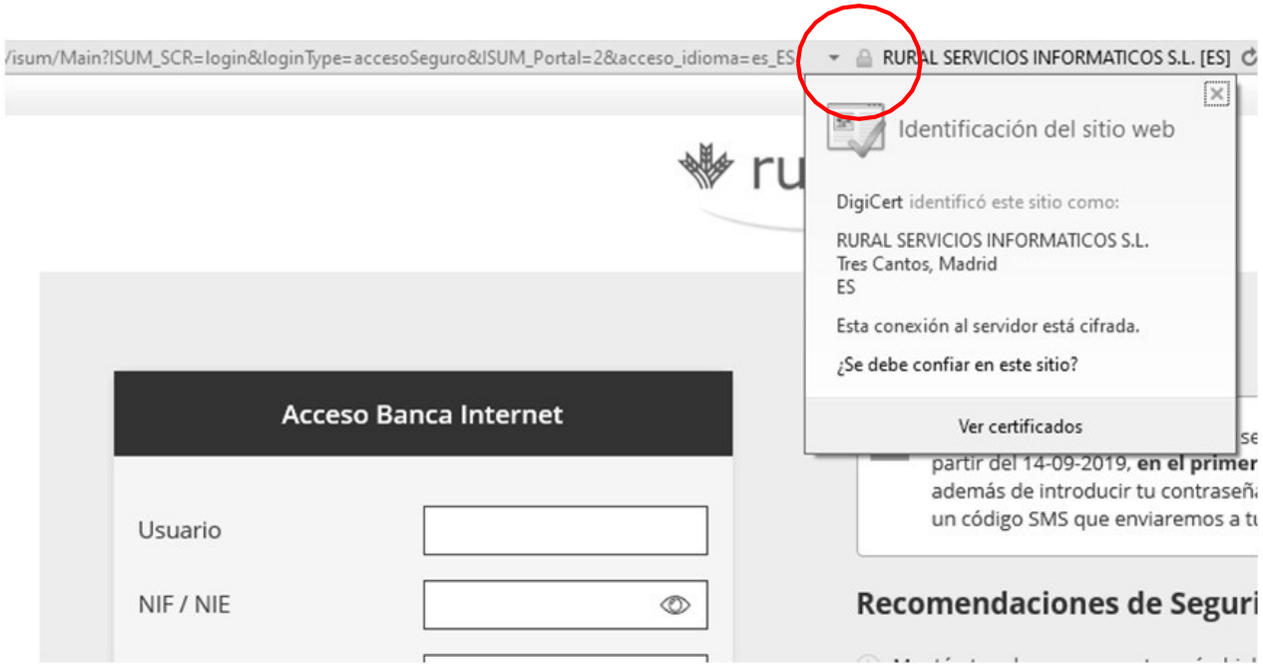
Validar que un sitio es Seguro HTTPS://

Validar que un sitio es Seguro HTTPS://



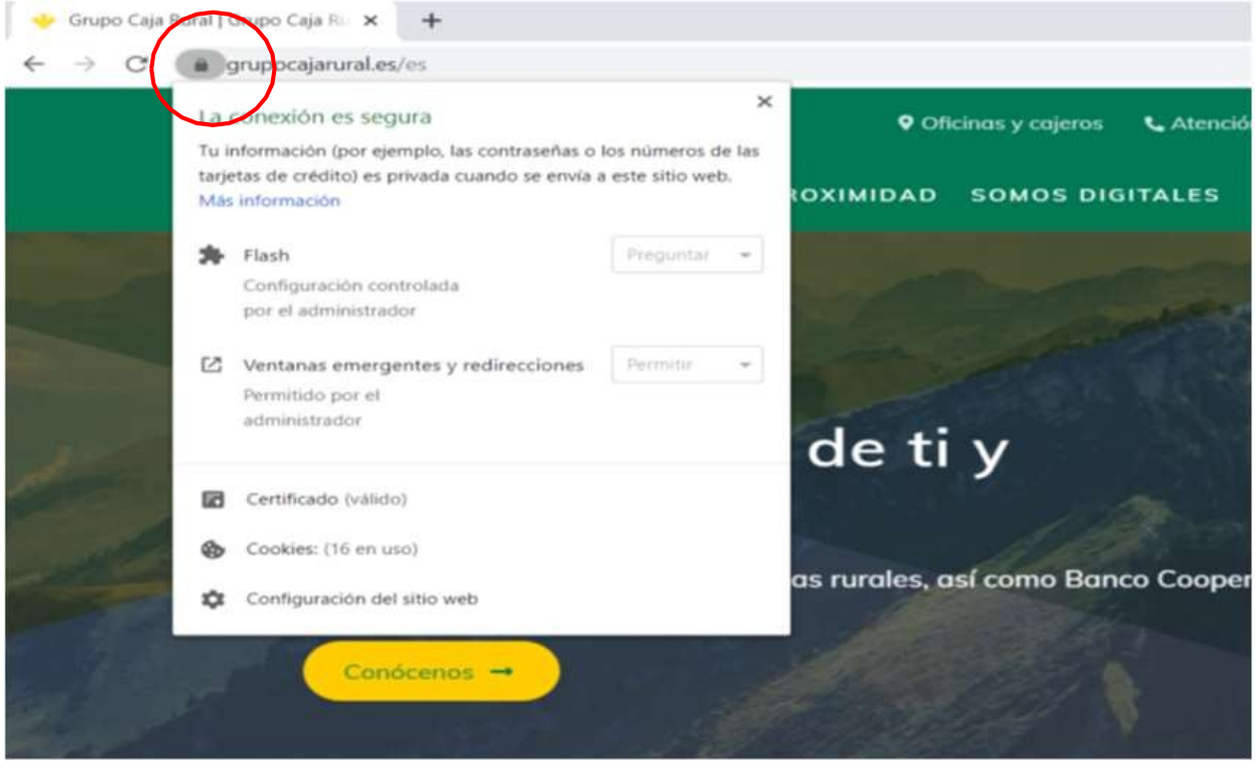
Validar que un sitio es Seguro HTTPS://

- **En Internet Explorer**



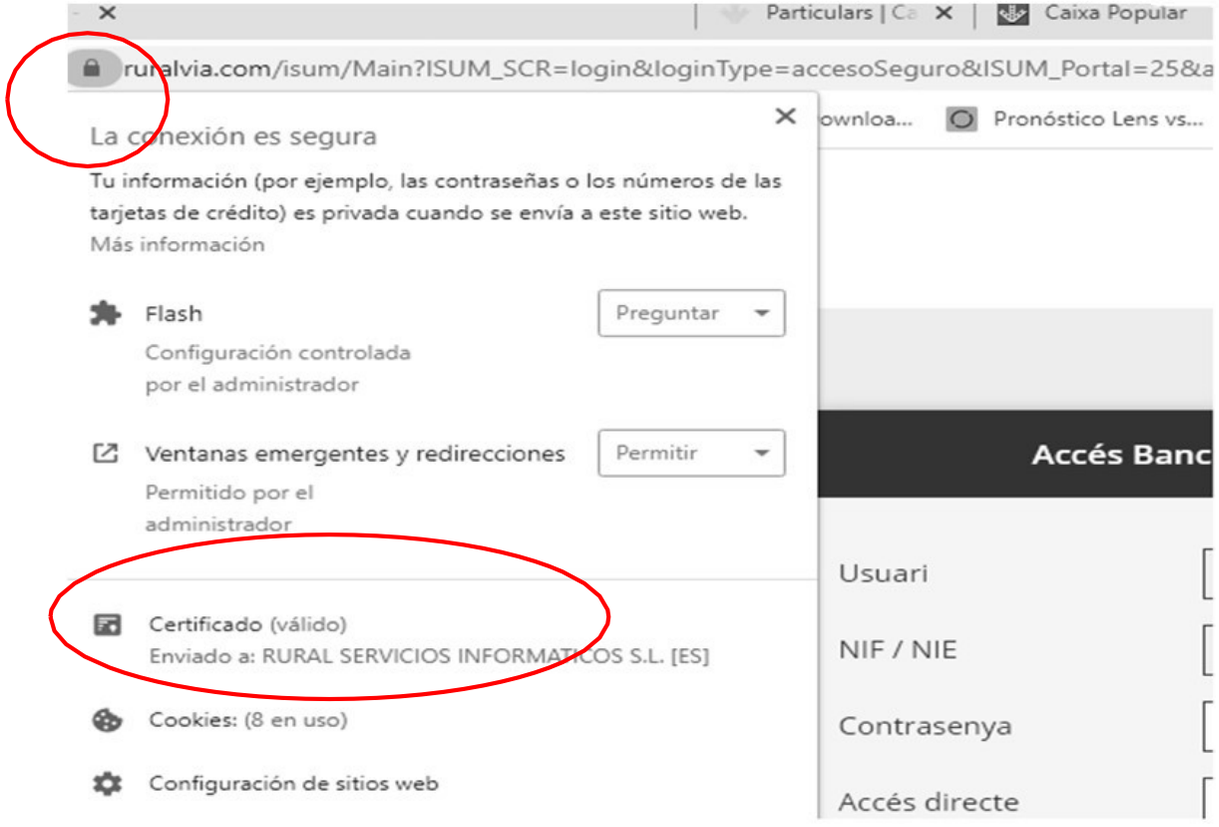
Validar que un sitio es Seguro HTTPS://

- **En Microsoft Edge**



Validar que un sitio es Seguro HTTPS://

- **En Google Chrome**



Regla de Oro para acceso a Banca Online y Organismos Oficiales

- **NUNCA acceder desde un enlace externo.**

✓ **Ni desde un enlace en un mensaje.**
✓ **Ni desde un enlace en otra pagina web.**

- **Siempre.**

✓ **Accederemos desde la web Oficial.**
✓ **Accederemos desde la APP Oficial.**

Contraseñas : Buenas Practicas

- **Si compartimos nuestras contraseñas están dejarán de ser secretas y por tanto perderán su utilidad. Debemos asegurarnos de lo siguiente:**

✓ **No debemos compartirlas con nadie.**
✓ **No debemos apuntarlas en papeles o post-it.**
✓ **No debemos escribir nuestras contraseñas en correos electrónicos ni en formularios web cuyo origen no sea confiable.**

- Usar una contraseña por cada servicio

✓ Corporativo
✓ Banca Electrónica.
✓ Compras Internet (Tarjeta Virtual)
✓ Redes Sociales.
✓ Aplicaciones personales.

Solo introduciremos nuestros email corporativo en las aplicaciones corporativas.

- Las contraseñas deben de ser robustas y NO USAR:

✓ **Palabras sencillas en cualquier idioma (palabras de diccionarios)**
✓ **Nombres propios, fechas, lugares o datos de carácter personal**
✓ **Palabras que estén formadas por caracteres próximos en el teclado.**

- **Fuerza Bruta:** Consiste en adivinar nuestra contraseña a base de ensayo y error. Los atacantes comienzan probando diferentes combinaciones con nuestros datos personales, en caso de conocerlos por otras vías. Luego, continúan haciendo combinaciones de palabras al azar, conjugando nombres, letras y números, hasta que dan con el patrón correcto.

- **Ataque por diccionario:** Los ciberdelincuentes utilizan un software que, de forma automática, trata de averiguar nuestra contraseña. Para ello, realiza diferentes comprobaciones, empezando con letras simples como “a”, “AA” o “AAA” y, progresivamente, va cambiando a palabras más complejas.

Importante usar contraseña Robustas para evitar ataques

Ranking de Contraseñas más usadas

Contraseña	Tiempo para descifrarla	RECUENTO
123456	< 1 Segundo	4.524.867
admin	< 1 Segundo	4.008.850
12345678	< 1 Segundo	1.371.152
123456789	< 1 Segundo	1.213.047
1234	< 1 Segundo	969.811
password	< 1 Segundo	710.321
qwerty	<1 Segundo	553.225

caixa popular

Importante usar contraseña Robustas para evitar ataques

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

En 2021 costaba 7 meses y en 2012 costaba 106 años.

Importante usar contraseña Robustas para evitar ataques

- Si tú me dices ven lo dejo todo.

Stmdvldt-3511

Importante usar contraseña Robustas para evitar ataques

¡Buena contraseña!

- Tu contraseña es resistente al pirateo.
- Tu contraseña no aparece en ninguna base de datos de contraseñas filtradas.

Tu contraseña puede ser descifrada con un ordenador común en...

33 siglos

En ese tiempo puedes ir y volver a la Luna 133 veces.

L05 NUM3R05 PU3D3N U71L1Z4R5E C0M0 L37R45, Y L4 FR453 R35UL74NT3 PU3D3 53R L31D4 51N MUCH0 E5FU3RZ0.

Importante usar contraseña Robustas para evitar ataques

LETRA	NUMERO
S	5
O	0
I	1
A	4
E	3

Importante usar contraseña Robustas para evitar ataques

Importante usar contraseña Robustas para evitar ataques

- ✓ **Voy a pasarmelo bien**

V0y4p454rm3lob13n

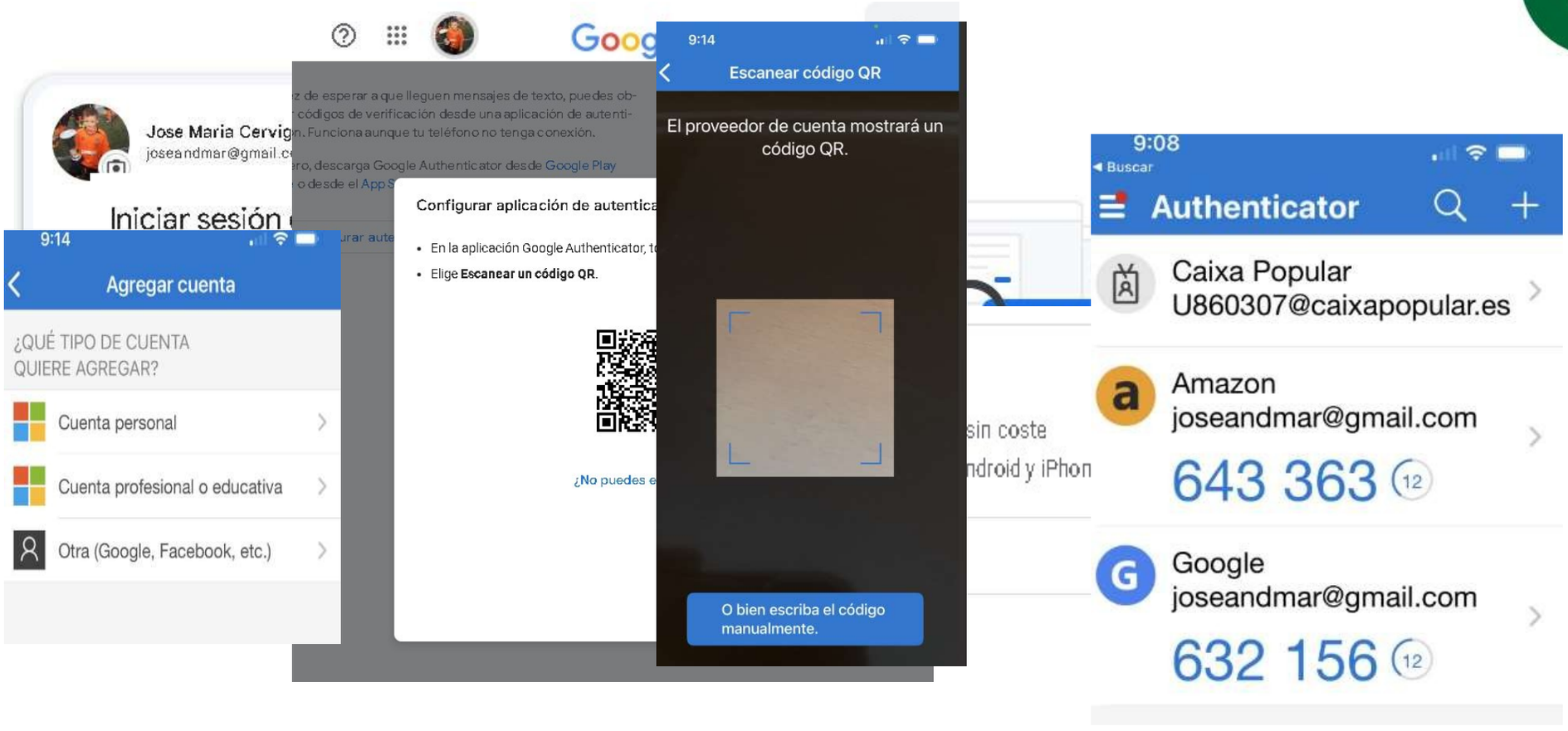
Importante usar contraseña Robustas para evitar ataques

MFA: Autentificación Multifactor

Microsoft Authenticator

Microsoft Corporation

MFA: Autentificación Multifactor GMAIL



- Tenemos que bloquear la sesión al ausentarnos del puesto de trabajo.

- Dejar un equipo sin protección durante el almuerzo, la comida, es equivalente a no utilizar contraseña.

Luego Vuelvo

Inversión en Tecnología

Tecnología	Inversión
Dominio Propio	40 Eu. Año
Correo Corporativo (Office 365) + App	80 Eu Usuario/año
Antivirus Profesional	70 Eu Usuario/Año
Copias de Seguridad fuera de línea(nube)	975 Eu + 1 TB nube(94Eu Anual)
Cortafuegos	980 € (hasta 25 usuarios)
SW con licencia	130 Eu puesto
Validación Usuarios y permisos	Configuración
NO USB	Configuración
Autentificación MFA	Configuración

Inversión

Simulación Primer Año	
Mano de Obra	600 Eu
Inversión Inicial	2.000 Eu
Total Inicial:	2.600 Eu
Coste por Empleado/Año	150 Eu

Total Inicial a 3 años	78 Eu/mes

Coste Diario	2,6 Eu

Coste Diario por Empleado	0,41 Eu

Por donde empezar: KIT DIGITAL

El objetivo de esta solución es proporcionar seguridad básica y avanzada para los dispositivos de tus empleados.

Importe máximo de la ayuda

- 0 < 3 empleados: 125€/dispositivo (hasta 2 dispositivos)
- 3 < 9 empleados: 125€/ dispositivo (hasta 9 dispositivos)
- 10 < 50 empleados: 125€/ dispositivo (hasta 48 dispositivos)

Funcionalidades y servicios

- **Antimalware:** tendrás a tu disposición una herramienta que analice tu dispositivo, su memoria interna y los dispositivos de almacenamiento externos.
  Antispyware: dispondrás de una herramienta que detecte y evite el malware espía.
  Correo seguro: tendrás herramientas de análisis del correo electrónico con las siguientes características:
  - **Antispam,** con detección y filtro de correo no deseado.
  - **Antiphishing,** con detección de correos con enlaces o malware que se sospecha sirvan para robar credenciales.

  Navegación segura: tendrás asegurado:
  - **Control de contenidos**.
  - **Antiadware** para evitar anuncios maliciosos.

  Análisis y detección de amenazas: serás capaz de conocer el comportamiento de las amenazas conocidas y nuevas.
  Monitorización de la red: tendrás herramientas que analizan el tráfico de red y te alerten de amenazas.
- **Configuración inicial y actualizaciones de seguridad:** dispondrás de una configuración inicial para su correcto uso, con las respectivas actualizaciones de firmas de malware y otros datos para detección de amenazas además de las actualizaciones de software de seguridad periódicas requeridas.
- **Requisitos especiales de formación:** dispondrás de formación para la configuración del software de seguridad, y tendrás un kit de concienciación en ciberseguridad para complementar la solución con habilidades de firewall humano.

“Completar el circulo ….”

caixa popular

CIBERSEGURIDAD FÁCIL: CÓMO DEFENDER A TU EMPRESA DE LAS AMENAZAS INFORMÁTICAS

Ciberseguretat. Solucions per a pimes i autònoms.

Enric Cerdà Moreno
Gestor de Segurs Empresa

OFICINA Acelera pyme
FEMEVAL
red.es
Fondos Europeos
Fondo Europeo de Desarrollo Regional
"Europa se siente"

HISCOX

Seguros Especializados

+120

Años de experiencia

+1 M

Negocios protegidos

14 países
3 continentes

2022

Premio Azul Innovación (NESE)

TOP 3 Compañías mejor valoradas (ADECOSE)

OFICINA Acelera pyme
FEMEVAL
red.es
Fondos Europeos
Fondo Europeo de Desarrollo Regional
"Europa se siente"

HISCOX

Panorama Ciberseguridad

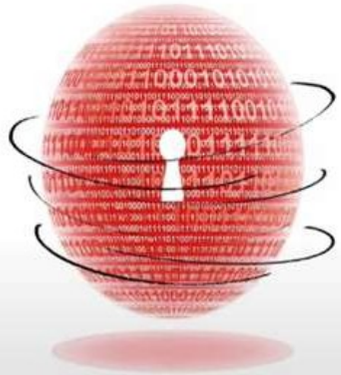
6º Informe ciberpreparación Hiscox - 2022

+50% Empresas atacadas en el último año

150% Aumento VS 2020

9/10 Vulnerabilidades x descuido humano

60% Empresas impactadas **Desaparecen** en 6 meses



Nivel de Preparación

2% Empresas Ciber Expertas

30% Empresas Ciber Novatas

caixa popular

OFICINA Acelera pyme

FEMEVAL

red.es Fondos Europeos

Fondo Europeo de Desarrollo Regional

"Europa se siente"

HISCOX

Servicio de respuesta a incidentes:

- Contención del ataque
- Asesoramiento Jurídico
- Gastos de notificación RGPD
- Cuidado de la imagen

1-CONTENCIÓN

Pérdidas derivadas de un ataque:

- Gastos de recuperación de datos o sistemas.
- Gestión y reembolso de rescate por extorsión.
- Pérdida de beneficios por interrupción.
- Pérdidas por ataque a su proveedor tecnológico.

2-PÉRDIDAS

3-FRAUDE TECNOLÓGICO

- Uso fraudulento de identidad electrónica.
- Robo electrónico de fondos.
- Modificación de precios online.
- Fraude en servicios contratados.
- Suplantación de identidad.

4-RESPONSABILIDAD CIVIL TECNOLÓGICA

Responsabilidad tecnológica.

- Gasto de defensa.
- Responsabilidad ante terceros por contenido digital.
- Sanciones administrativas en protección de datos y Sanciones PCI.

PREVENCIÓN

Servicios de prevención (incluidos):

- Academia Cyber para empleados.
- Análisis de vulnerabilidad Red e Internet.
- Antivirus gratuito.
- Copias de seguridad 20 gb.
- Servicio de noticias y alertas.