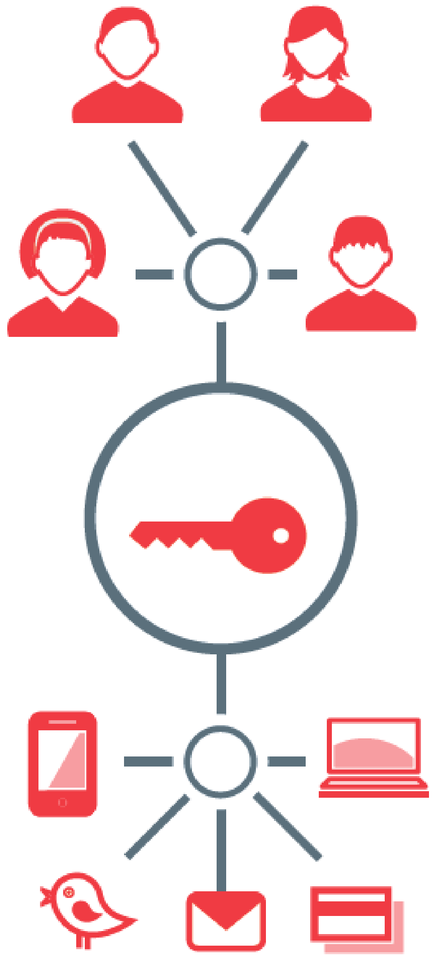
CIBERSEGURIDAD

SOLUCIONES Y SERVICIOS IT PARA EMPRESAS

Dagram-BSA-Confidencial



Jornada de concienciación de CIBERSEGURIDAD

CONSEJOS PRÁCTICOS PARA PROTEGERNOS DE LAS CIBERESTAFAS

Octubre 2025

ÍNDICE

01

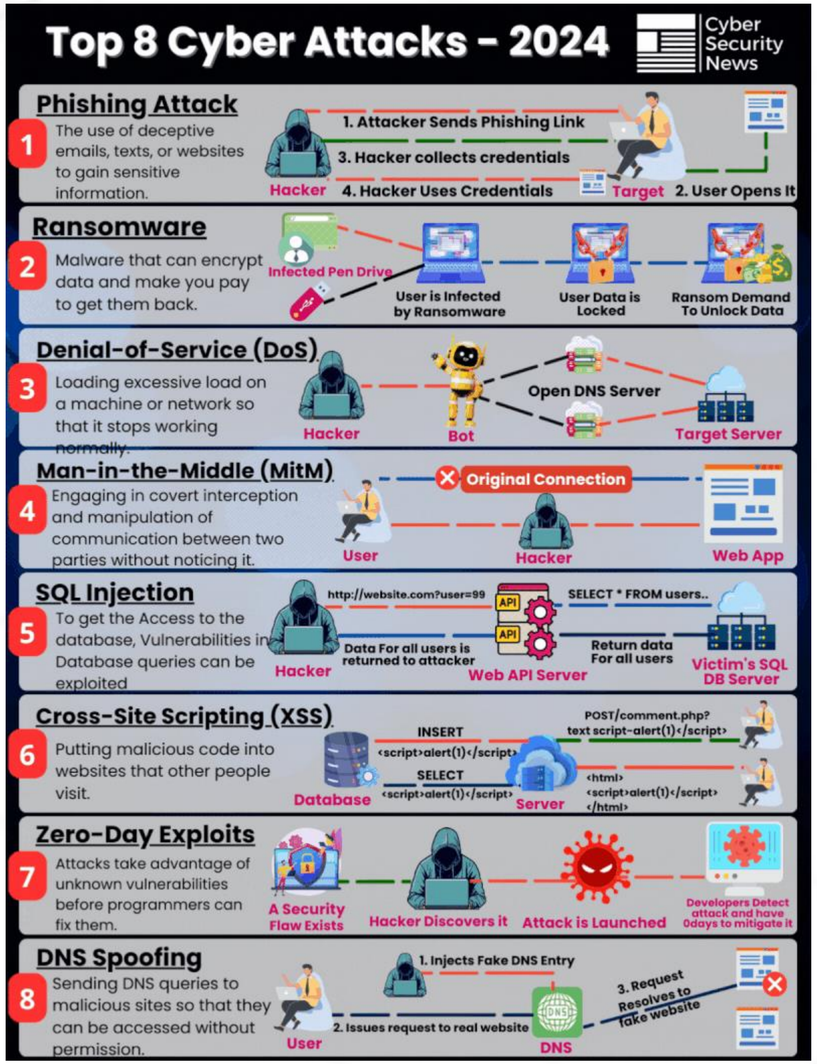
¿Por qué es importante hablar de CIBERSEGURIDAD?

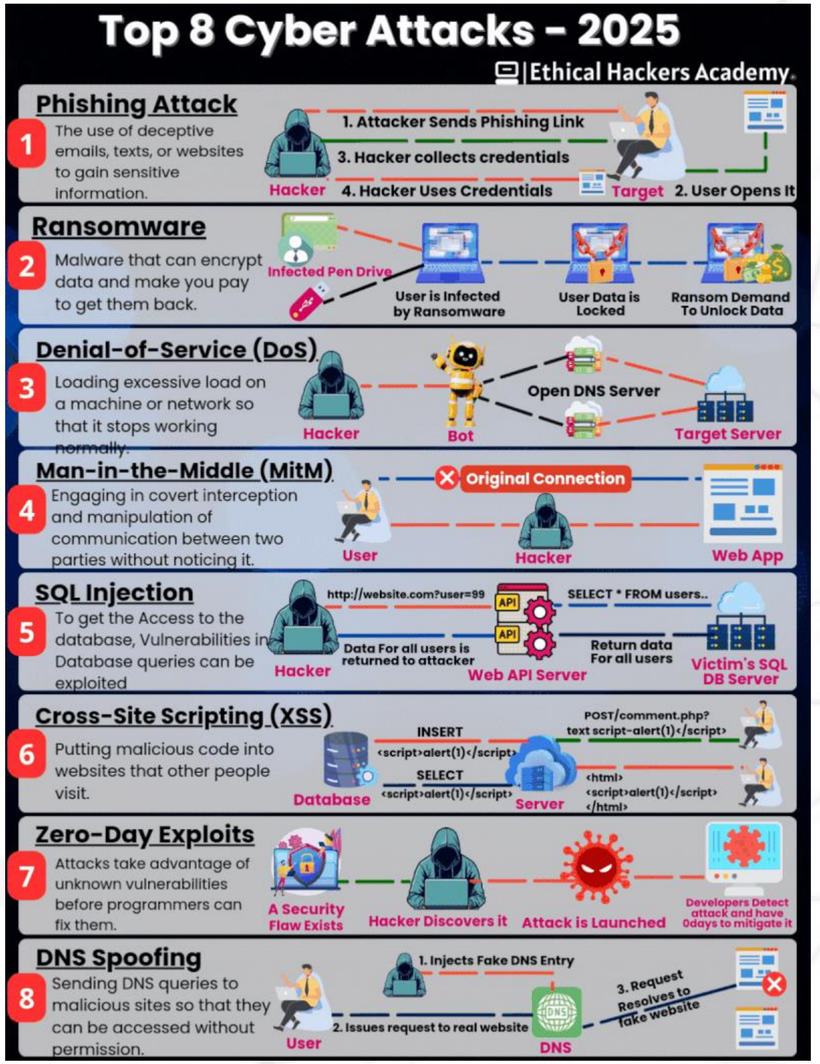
Dependemos cada vez más de la tecnología y la digitalización en nuestro día a día

- Todos utilizamos **contraseñas, redes Wi-Fi, redes sociales, banca online, dispositivos móviles**, etc.
- Aumento del **teletrabajo**, la **inteligencia artificial** y el **dispositivos con internet** (IoT) amplían la superficie de ataque.
- Un error humano (clic en un enlace falso, compartir información sin pensar, usar contraseñas débiles) puede abrir la puerta a ataques más grandes.

La ciberseguridad ya no es solo cosa de "informáticos", sino de todos.

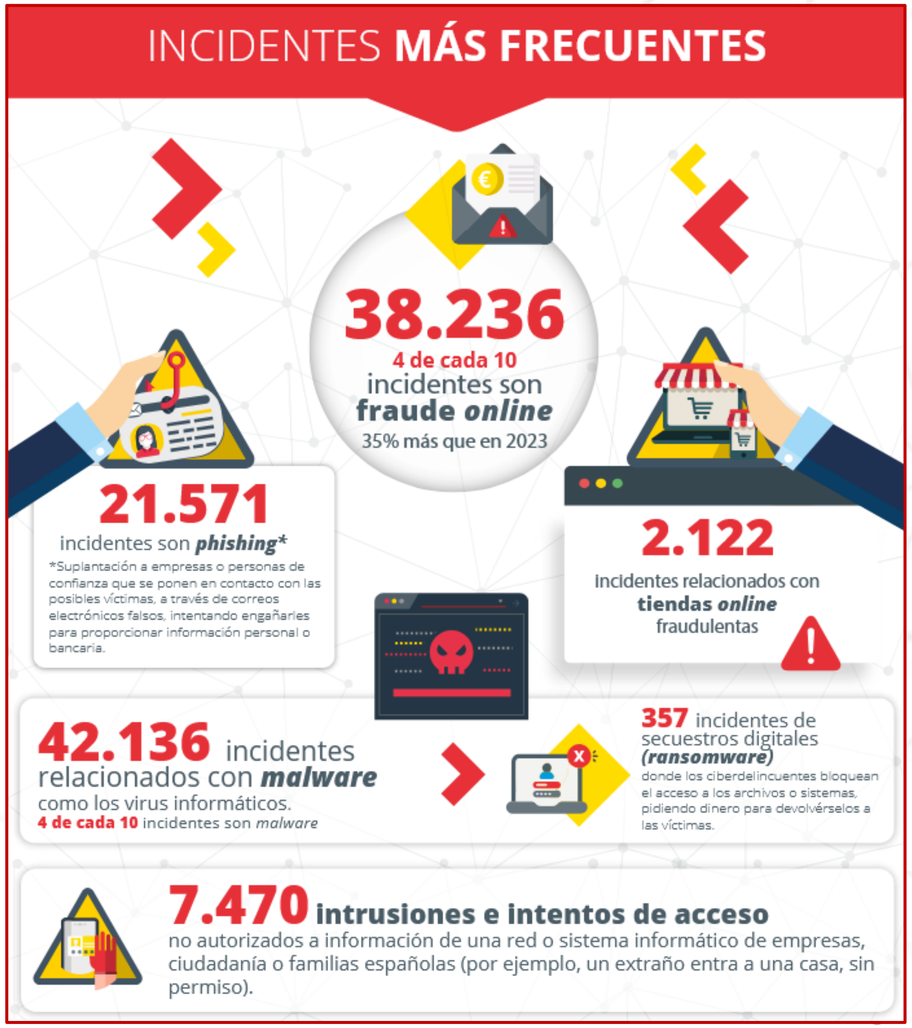
Estadísticas





Estadísticas

balance de ciberseguridad



Fuente: *Balance de Ciberseguridad de Incibe 2024:https://www.incibe.es/sites/default/files/Comunicaci%C3%B3n_2025/Infograf%C3%ADa_BalanceCiberseguridad_INCIBE_2024_web.pdf*

02

Ingeniería social

¿qué es?

Técnica que emplean los ciberdelincuentes para **ganarse la confianza** del usuario y conseguir así que haga algo bajo su **manipulación y engaño**.

PREMISA BÁSICA

Es más fácil manejar a las personas que a las máquinas.

Ingeniería social

selección de un objetivo

Datos profesionales

LinkedIN: Experiencia profesional, relaciones con clientes y proveedores

Información del puesto que ocupa: ¿Tendrá capacidad de hacer o encargar una transferencia? ¿Puede tener permisos de administración en el sistema informático?

Búsqueda en Google: entrevistas, artículos, nombramientos...

Datos personales

Redes sociales: vacaciones, fotografías, amistades, familia, perfiles mal configurados,... ¿Parece manipulable? Retweets, publicaciones en muros, foros,...

Búsqueda en Google: direcciones de correo electrónico, datos personales, intereses, hobbies,...

Vulneraciones previas

Búsqueda en páginas especializadas: ¿Existe vulneración previa? HaveIbeenPwned, Intelligence X,...

Búsqueda en foros de la Darkweb

Canales de Telegram

Credenciales publicadas: gratuitas o en venta

02

Ingeniería social

La estafa del falso Brad Pitt

- Una mujer francesa (Anne) es engañada **a lo largo de meses** por un supuesto Brad Pitt, ganándose su **confianza**.
- En primera instancia es la supuesta **madre de Brad** (Jane Etta Pitt) quien entabla amistad con Anne, posteriormente es directamente "Brad Pitt".
- Utilizan todo tipo de métodos, imágenes y videos falsos (**deepfake**) donde l víctima veía al actor hablándole directamente.
- El estafador llegaba a enviar **regalos de lujo** a Anne.
- En un momento dado y utilizando la excusa de la **separación de Angelina Jolie** y que está había congelado las cuentas bancarias, manifiesta que no puede sacar dinero del banco y lo necesita urgentemente por temas de salud. Está ingresado.
- **Anne duda, su hija le dice que la están engañando**, pero Anne le decía "Ya verás cuando esté aquí en persona".
- Al final Anne transfiere un total de **830.000 €** a una cuenta de Turquía.
- Finalmente, al verle aparecer en los medios de comunicación completamente sano y con una nueva pareja asume el engaño.

El 'falso Brad Pitt' español

La estafa del 'falso Brad Pitt' es un método que cada vez más delincuentes utilizan para conseguir el dinero de sus víctimas. Hace tan solo cuatro meses dos mujeres **perdieron más de 300.000 euros** en España al pensar que estaban hablando con el actor real.

02

¿CÓMO PROTEGERNOS?

egosurfing

Todo lo que publicamos en Internet; fotos, vídeos, opiniones, etc., e incluso lo que otros publican sobre nosotros, incluyendo documentación o publicaciones oficiales, donde aparece información sobre nosotros, permanece en la Red. Esa es nuestra **huella digital** y puede ser utilizada para dañar tanto nuestra reputación, como servir de base a un ataque más ambicioso y dañar todo un sistema informático corporativo.

Al hacer click en un enlace sospechoso podemos infectar un sistema informático o facilitar información (usuario, contraseña, DNI, datos bancarios, etc).

Es conveniente intentar saber qué sabe Internet de nosotros (datos corporativos y personales).

BUSCAR QUÉ SABE GOOGLE DE NOSOTROS

02

¿CÓMO PROTEGERNOS?
redes sociales

PROTECCIÓN DE LA IDENTIDAD Y LA INFORMACIÓN PERSONAL

- Evitar compartir datos sensibles como dirección, número de teléfono, centro educativo o lugar de trabajo.
- No publicar documentos personales (DNI, pasaporte, tarjetas, boletos de viaje, etc.).
- Usar nombres de usuario y fotos de perfil que no revelen demasiado sobre tu vida privada.

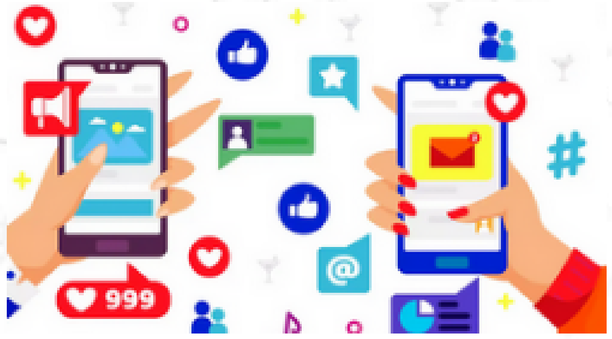
CONFIGURAR LAS OPCIONES DE PRIVACIDAD

- ¿Cómo pueden encontrarte y ponerse en contacto contigo los demás?
- Visibilidad del perfil.
- Registro de actividad.
- Eliminar cuentas de redes sociales que ya no usemos.

INCIBE: https://www.incibe.es/ciudadania/blog/consejos-para-proteger-tu-privacidad-online

¿CON QUIÉN INTERACTUAMOS?

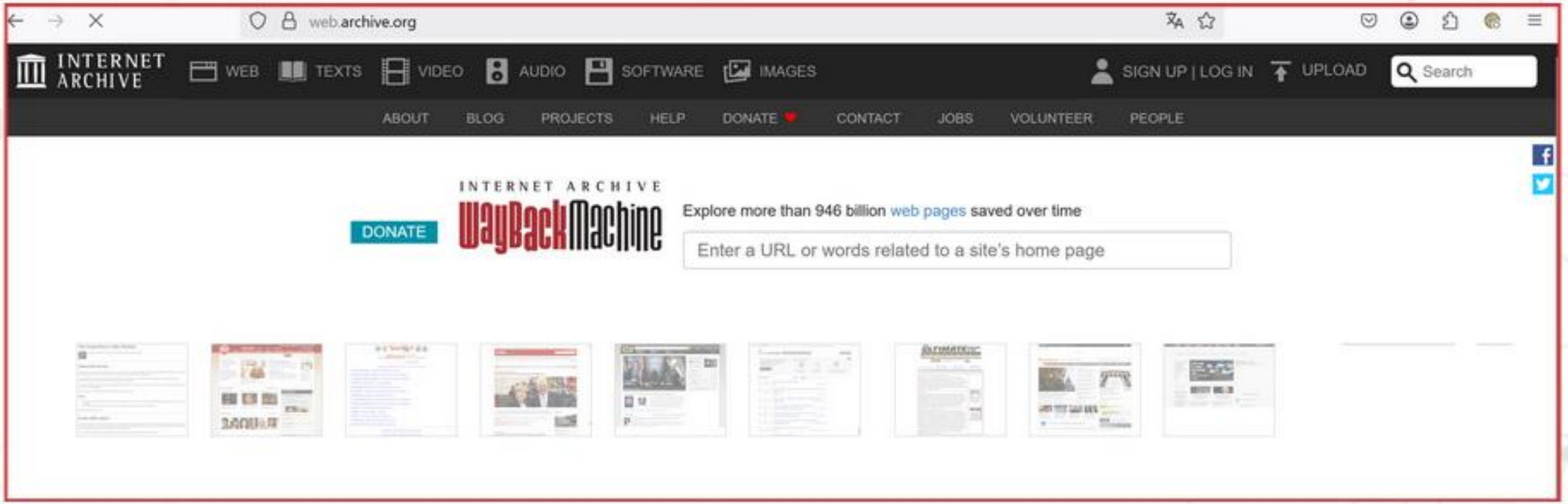
- Verificar la identidad de la persona/empresa.
- No compartir información personal con desconocidos.
- Si encontramos un perfil falso en una red social, denunciarlo.



02

¿CÓMO PROTEGERNOS?

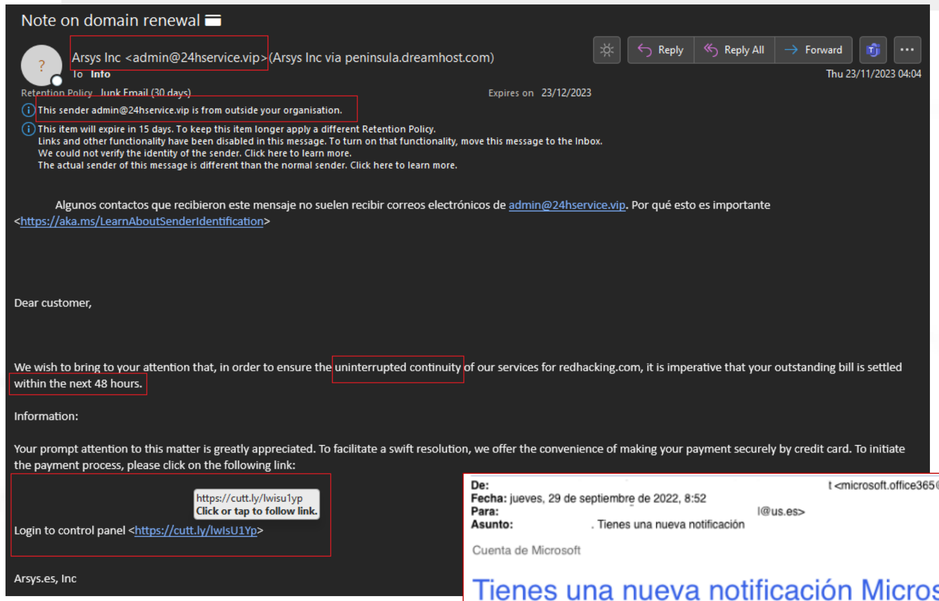
dificultad de eliminar datos de internet

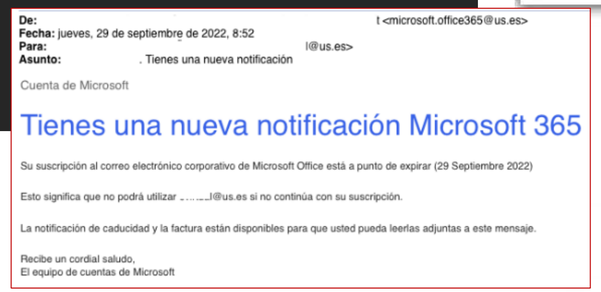


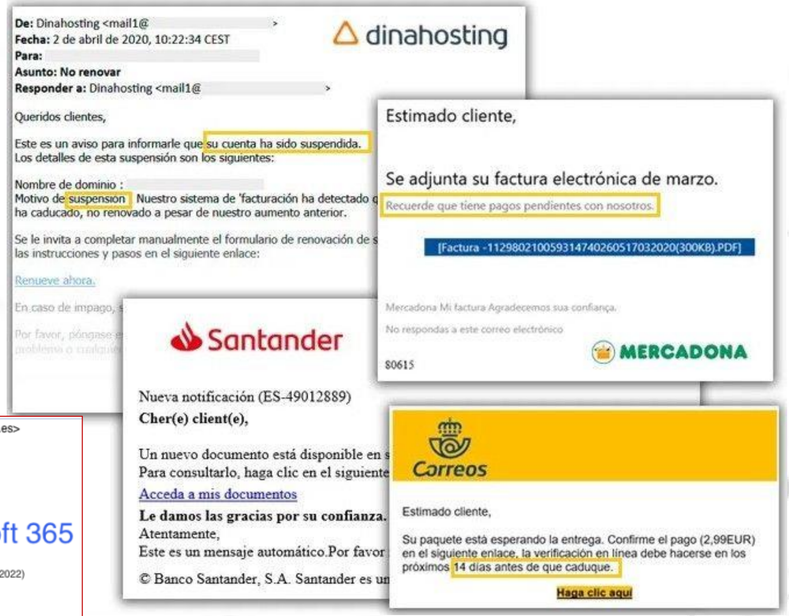
web.archive.org

Phishing

El ***PHISHING*** es una técnica de ingeniería social que consiste, generalmente, en el envío de **correos electrónicos** que **suplantan la identidad** de organizaciones o personas con el objetivo de **engañar, presionar y manipular** a las personas para que envíen información confidencial o se descarguen malware a través de un archivo adjunto.







03

Analizando un correo de phishing

03

Analizando un correo de phishing

Analizando un correo de phishing

03

Analizando un correo de phishing

Festes de maig

MB

Màgic Badalona <comunicacion-magicbadalona@soportemail.net>

Para

Responder

màgic badalona

VIU LES FESTES DE MAIG

al Màgic Badalona!

Amb motiu de les Festes de Maig de Badalona, el centre comercial MÀGIC BADALONA vol reconèixer el treball de totes les persones que formeu part de l'àmbit sanitari de la ciutat.

TICKET

VOLEM OBSEQUIAR-VOS AMB

100 entrades dobles per anar al cinema OCINE Màgic

A més, tots els participants accediran a un pack de descomptes exclusius, que inclou:

- ***Fins a un 30% de descompte en restaurants adherits***
- ***Promocions en pistes de pàdel***
- ***Avantatges en aparcament i altres serveis del centre***

REGISTRA'T I REBRÀS MÉS DETALLS DE LA PROMOCIÓ

Accedeix al registre

Vine a descobrir-nos

Tot el que necessites està a Màgic Badalona

màgic badalona

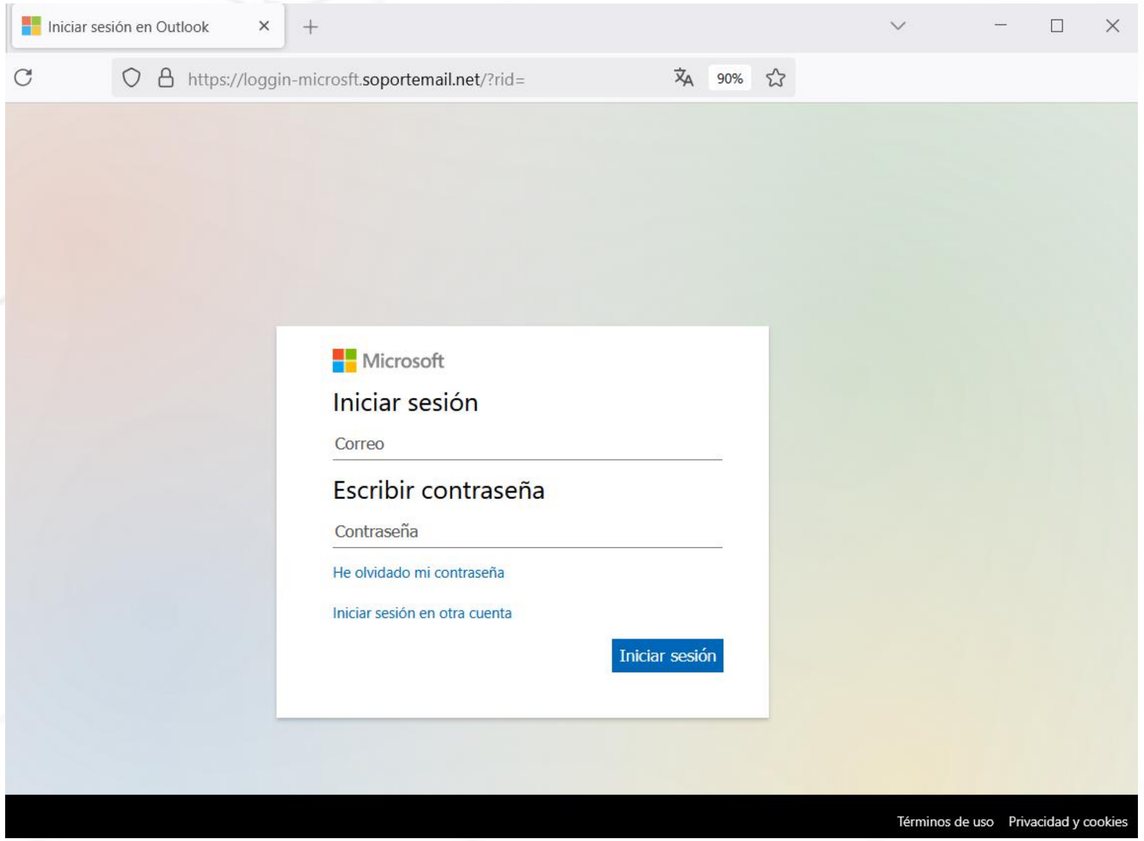
- ✓ Gratis
- ✓ Urgencia
- ✓ Petición de registro

Analizando un correo de phishing

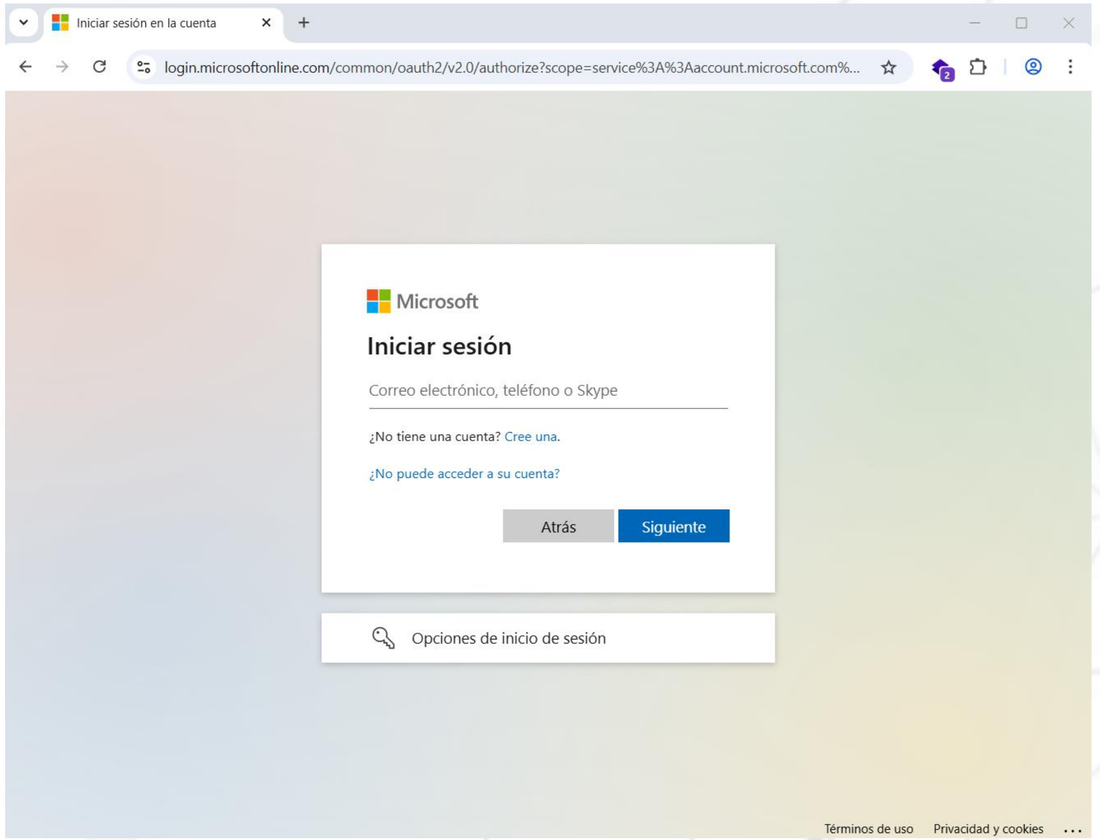
03

Analizando un correo de phishing

PÁGINA FALSA CREADA PARA LA CAMPAÑA

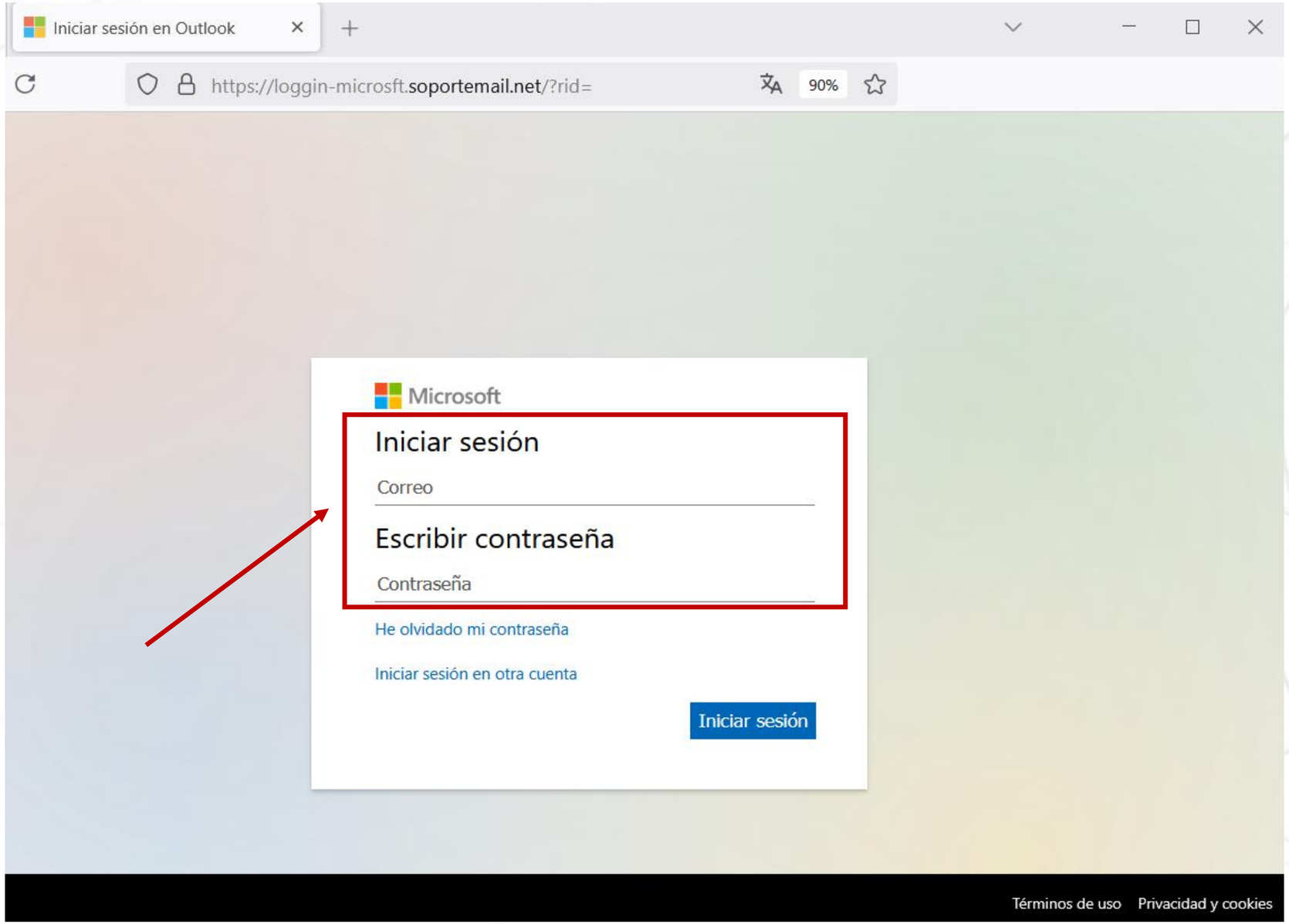


INICIO DE SESIÓN EN MICROSOFT



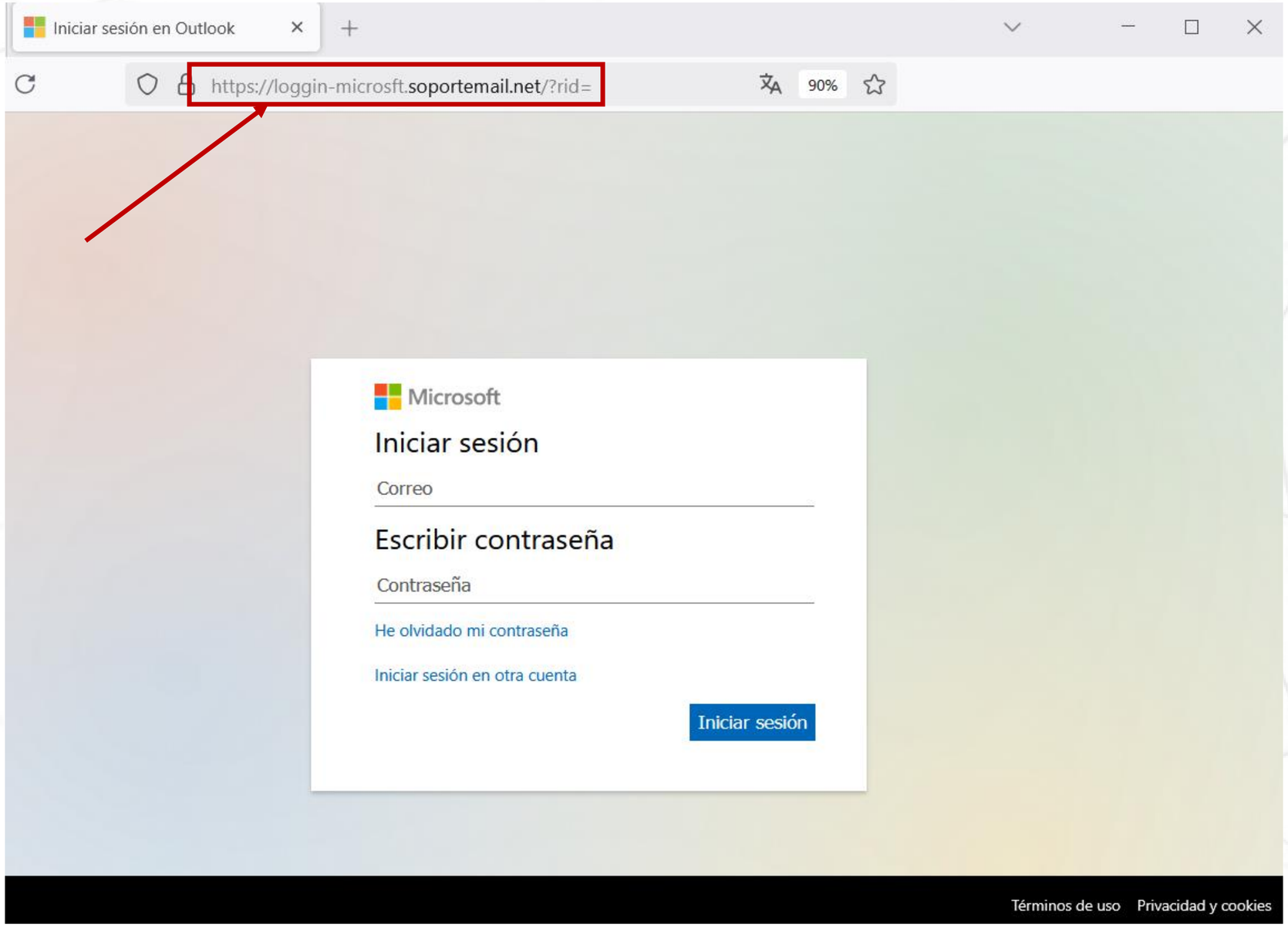
03

Analizando un correo de phishing

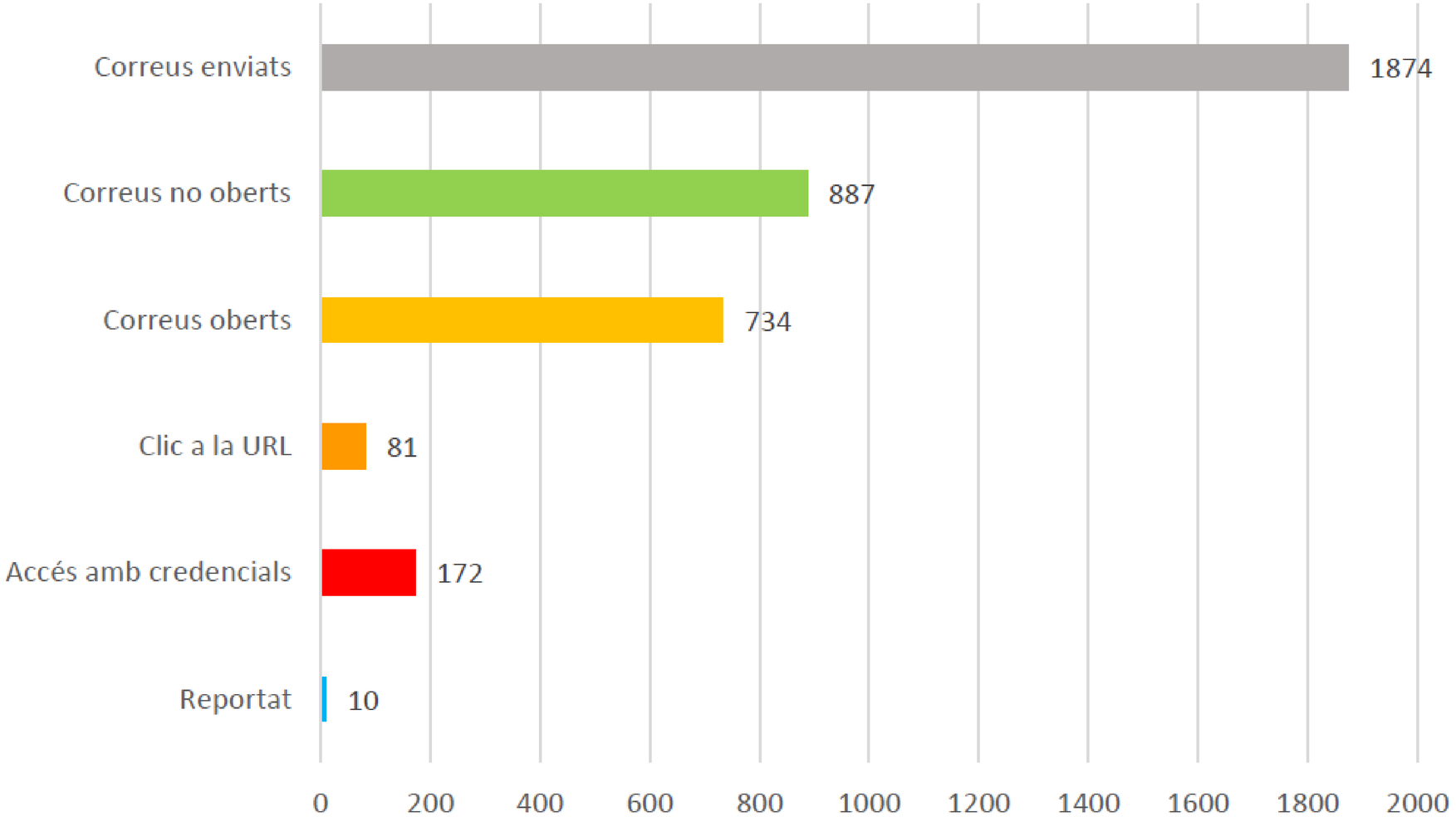


03

Analizando un correo de phishing



Resultados phishing



03

¿Cómo nos ciberatacan cada día?

SMISHING

Envio de un **SMS** simulando ser una entidad legítima con el objetivo de robar información privada o realizar un cargo económico a un usuario.

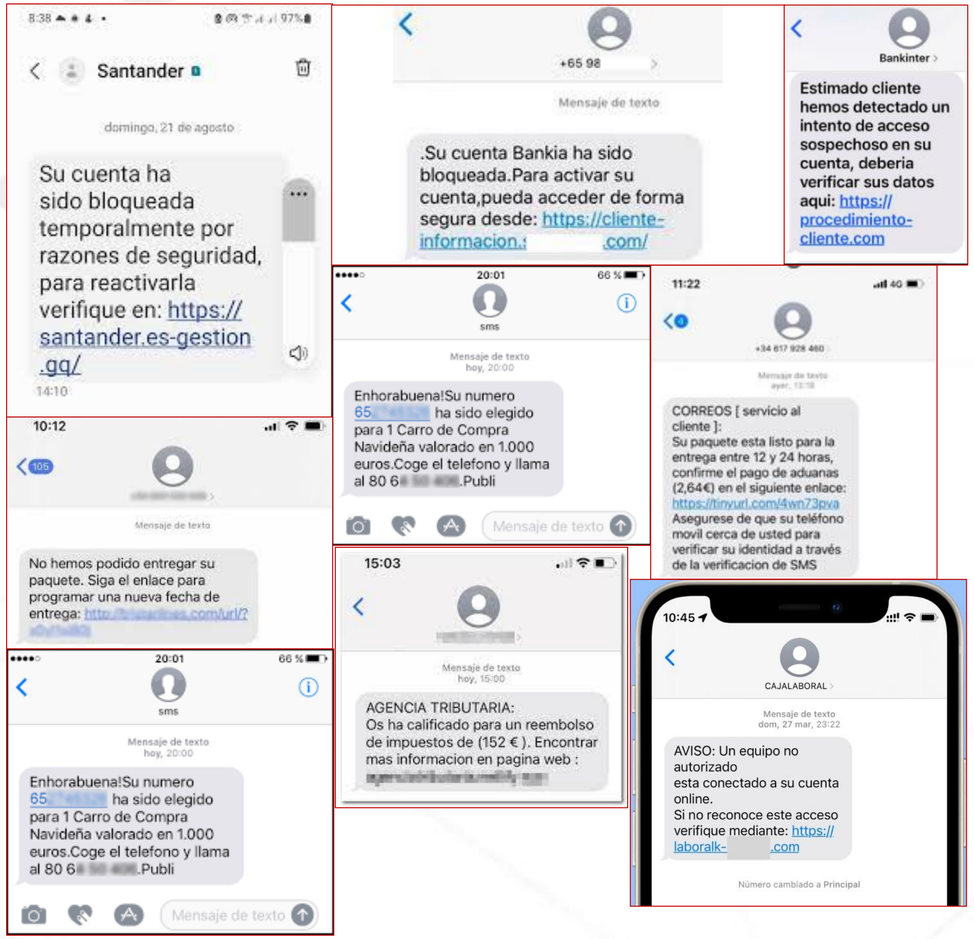
VISHING

Fraude que se realiza a través de una **llamada telefónica** con el objetivo de conseguir los datos

ATAQUES EN REDES SOCIALES

Usan perfiles, mensajes o publicaciones manipuladas en redes sociales para engañar a usuarios, robar credenciales o difundir malware y desinformación.

Ejemplos SMISHING



- El servicio se interrumpirá o ha sido interrumpido. **Es urgente.**
- Es una **oferta demasiado golosa.**
- Envía a un enlace de panel de control con una **dirección URL acortada. (https://cutt.ly….), no se ve dónde va realmente.**
- Nos **redirige a una página web** en la que se nos pide datos (**credenciales**).

https://www.incibe.es/aprendeciberseguridad/smishing

Dagram-BSA-Confidencial

Casos reales VISHING

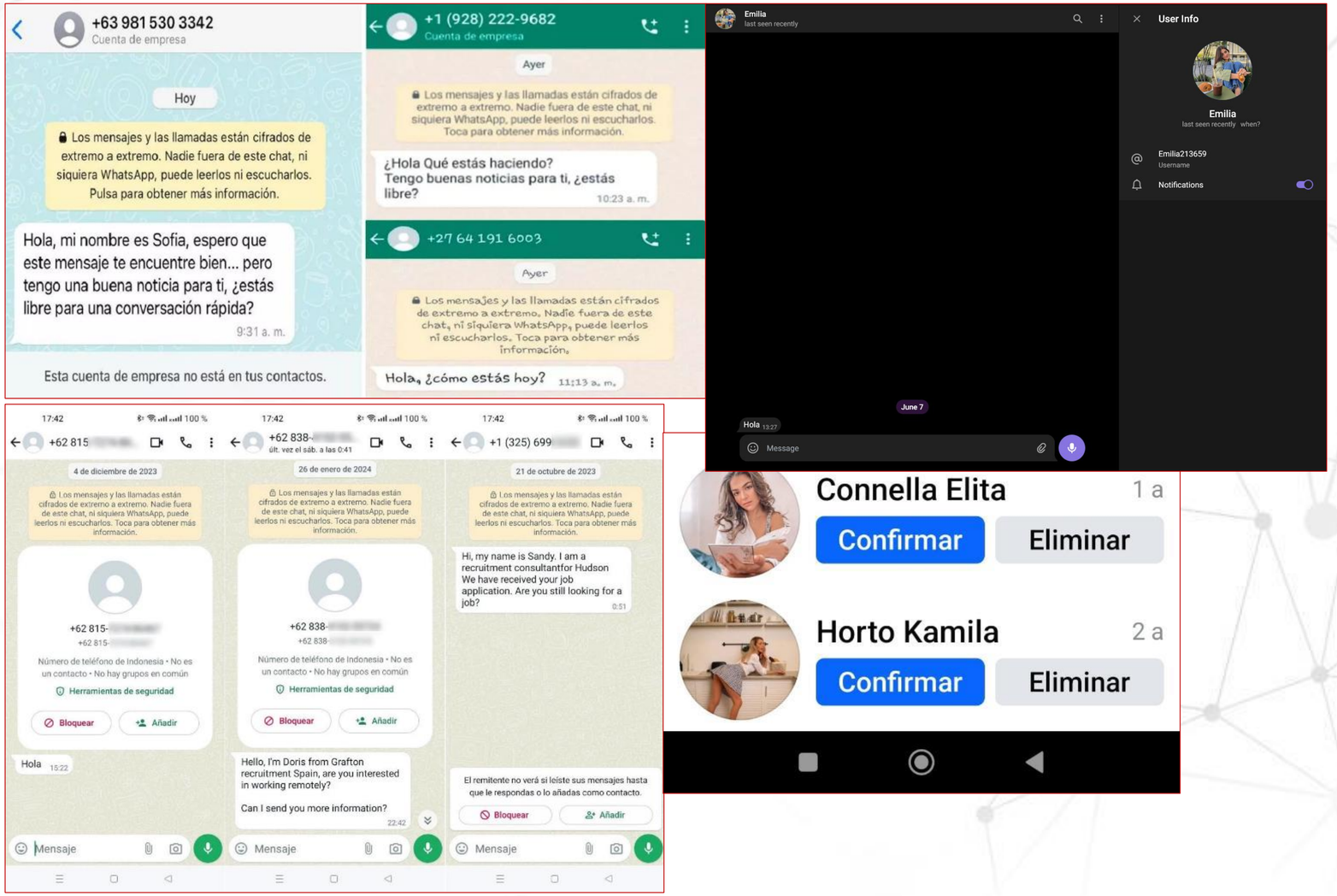
La llamada del SAT de Microsoft

Microsoft nunca te llama a casa ni a tu móvil.

No dejes a nadie conectarse a tu ordenador si no es de confianza.

https://support.microsoft.com/es-es/windows/prot%C3%A9jase-de-las-estafas-del-soporte-t%C3%A9cnico-2ebf91bd-f94c-2a8a-e541-f5c800d18435

Ataques en mensajerías (WhatsApp, Telegram, Redes Sociales...)



04

Otros vectores de ataque

REDES WIFI

WIFI PÚBLICAS (aeropuertos, hoteles, restaurantes,...) son de fácil suplantación. Interceptan información como contraseñas de acceso, cuentas bancarias, etc.

RECOMENDACIÓN

- **VPN**
- **Conexión de datos con nuestro móvil**

USB

Pueden contener virus o pueden esconder un pequeño chip que emula un teclado con memoria, de manera que es capaz de hacer lo que se le indique (parar antivirus, robar contraseñas, enviarlas, etc.)

RECOMENDACIÓN

- **No introducir USB personales en dispositivos de empresa**
- **No confiar en USB que encontremos por la calle**

APLICACIONES MÓVILES

Aplicaciones que se cierran solas, publicidad intrusiva donde no es habitual, menús extraños, consumo excesivo de bateria...

RECOMENDACIÓN

- **Tiendas oficiales exclusivamente**
- **Fuentes legítimas y software actualizado**
- **Revisar y dar los permisos estrictamente necesarios para el uso de la APP**

CÓDIGOS QR

El problema no es el hecho de escanear el código QR, sino en lo que se esconde detrás de él: descarga de malware, redirige página web fraudulenta (suplantación), etc.

RECOMENDACIÓN

- **Utilizar app que permita ver el enlace al que redirecciona**
- **Comprobar que no se ha suplantado con una pegatina el QR original**

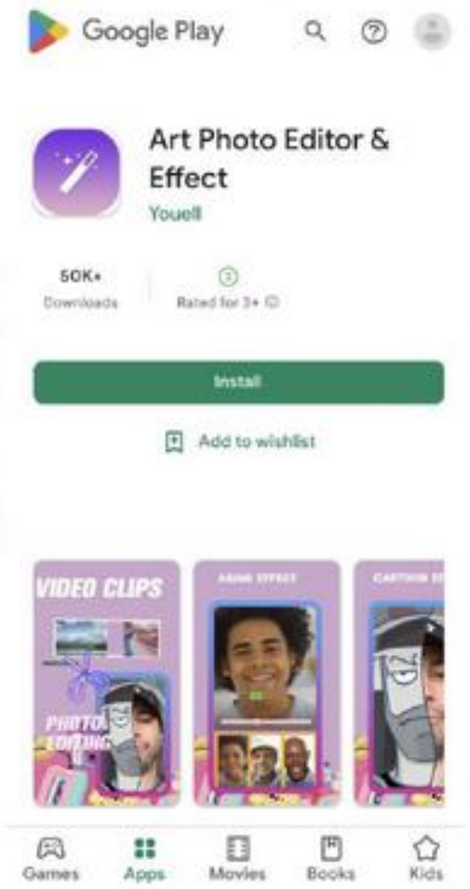
04

Otros vectores de ataque

ejemplos

BAD USB

APP MALICIOSA



CÓDIGO QR

Otros vectores de ataque

ejemplos

“Ataque” a través de Código QR

05

Medidas para protegernos
evitar ciberestafas

- VERIFICA CON QUIÉN ESTÁS HABLANDO
- NO FACILITES TUS CREDENCIALES A NADIE
- NO HAGAS CLICK EN ENLACES SOSPECHOSOS
- DESCONFÍA DE GRANDES REBAJAS O REGALOS
- NO COMPARTAS DATOS PERSONALES
- NO DESCARGUES ARCHIVOS EXTRAÑOS

Medidas para protegernos

el doble check

No dejarse llevar por las prisas, si nos piden algo demasiado urgente o demasiado goloso (¡*Cuidado*!)

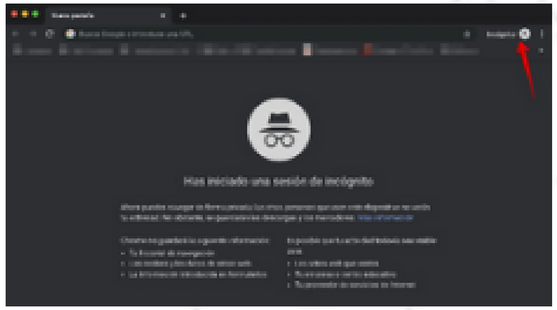
En la vida privada:

- **Palabras clave con familiares/amigos.**
- **Llamar personalmente a quien nos pide interactuar (Banco, familiar, etc.).**

En la vida profesional:

- **Palabras clave con CEO, CFO, personal de contabilidad, facturación.**
- **Pedir/cotejar siempre las cuentas bancarias (certificados de titularidad).**
- **No saltarse los circuitos/protocolos establecidos (comprobar siempre).**

Medidas para protegernos
navegación de incógnito



¿ La navegación en modo incógnito nos protege ?

PROS:

- **En un dispositivo compartido no registra el historial de navegación, cookies, etc.**
- **Al cerrar el navegador se eliminarán las cookies (previene posteriores publicidades, etc).**
- **Puedes abrir sesión en el mismo sitio web con varias cuentas**
- **Se ejecuta habitualmente sin extensiones de navegador.**

CONTRAS:

- **Sigues pudiendo ser rastreado (la huella en Internet no se borra). Si pretendes saltarte las normas o protecciones de la empresa así, NO FUNCIONA.**
- **Los registros de acceso tanto en las empresas como en los proveedores de Internet siguen siendo efectivos, ahí *NO SE ES ANÓNIMO*.**

NO TE PROTEGE NI A TI NI A LA EMPRESA DE AMENAZAS CIBERNÉTICAS

Enlaces de interés: Egosurfing

1. Configurar las opciones de privacidad (https://www.incibe.es/ciudadania/blog/consejos-para-proteger-tu-privacidad-online) en las redes sociales. Y en LinkedIN (https://www.incibe.es/ciudadania/blog/sabes-como-proteger-tu-privacidad-en-linkedin)
2. Si encontramos un perfil falso en una red social, denunciarlo.
    1. Facebook (https://es-es.facebook.com/help/306643639690823)
    2. Instagram (https://es-es.facebook.com/help/instagram/370054663112398?helpref=hc_fnav)
    3. X (Twitter) (https://help.x.com/es/safety-and-security/report-x-impersonation)
3. Ejercer el derecho al olvido (https://www.incibe.es/ciudadania/blog/ejerciendo-el-derecho-al-olvido) en buscadores
    1. Google (https://reportcontent.google.com/forms/rtbf)
    2. Yahoo (https://io.help.yahoo.com/contact/index?page=contactform&locale=es_ES&token=Zh%2FBBVqXzLHIlbokbUqVWTUbuuQeXGkGFw6kaYtcsz3bJLmIlI3EUv0z8vEZZIiUaVM%2FeyBEjFUCaMU2WNilF1pt08EKxz55Rcv1x17V0EmPwqCwTMq3EFzwfnJNrIXz0JmkcIODVsGATkR7pX7Nwg%3D%3D&selectedChannel=email-icon&yid=)
    3. Bing (https://www.bing.com/webmaster/tools/eu-privacy-request)
4. Derecho al olvido en redes sociales
    1. Eliminar cuenta de Facebook (https://www.facebook.com/help/250563911970368)
    2. Eliminar cuenta de Instagram (https://es-la.facebook.com/help/instagram/139886812848894?helpref=related)
    3. Eliminar cuenta de Twitter (https://help.twitter.com/es/managing-your-account/how-to-deactivate-twitter-account)
    4. Eliminar cuenta de TikTok (https://support.tiktok.com/es/my-account-settings/delete-account-es)

    Si no conseguimos hacerlo nosotros mismos hay servicios de pago
    - Incogni (https://incogni.com/)

Dagram-BSA-Confidencial

Enlaces de interés

- Analiza archivos, dominios, IP y URL para detectar malware: https://www.virustotal.com/
- Comprobar si la dirección de correo electrónico se ha visto vulnerada y está en una brecha de Seguridad. https://haveibeenpwned.com/
- Datos personales publicados en Internet: https://www.malwarebytes.com/digital-footprint-app

Programas recomendados

- Gestor de contraseñas de pago: Keeper Security https://www.keepersecurity.com/es_ES/
- Gestor de contraseñas de pago: https://1password.com/es
- Gestor de contraseñas gratuito: Bitwarden: https://bitwarden.com/pricing/
- Gestor de contraseñas gratuito: Keepass https://keepass.info/
- Antivirus per móvil: Kaspersky: https://www.kaspersky.es/free-antivirus
- Antivirus per móvil: Malware Bytes: https://es.malwarebytes.com
- VPN Gratuita: https://www.gethotspotshield.com/free-vpn/
- VPN pago: https://nordvpn.com
- VPN pago: https://esp.windscribe.com/

Dagram-BSA-Confidencial

Dagram-BSA-Confidencial

Contacto

Descubre más sobre Dagram en nuestra web o en redes sociales.

Contacta con nosotros si tienes cualquier duda sobre tu proyecto.

C/ de la Pau, 12 Ed. Capitanía Pl. 1
08930 Sant Adrià de Besos

www.dagram.com

@Dagram_TI

@dagram

OFICINA BARCELONA

C/ de la Pau, 12 Ed. Capitania Pl. 1
08930 Sant Adrià de Besos
+34 933 502 999

OFICINA MADRID

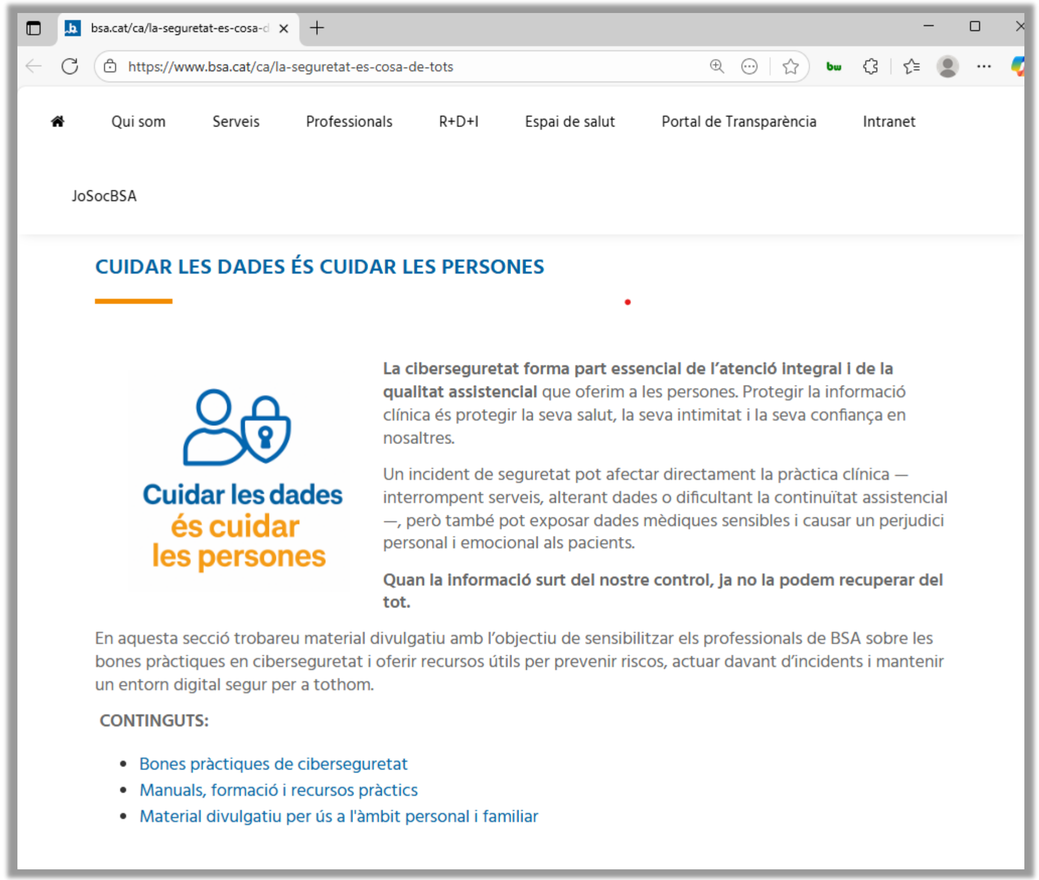
Sierra de Cazorla, 1
28290 Las Rozas de Madrid
+34 916 033 513

OFICINA PALMA

C/ Guatemala, 3
07014 Palma, Illes Balears
+34 971 498 476

BSA: Cuidar les dades és cuidar les persones

Saber afrontar
positivament els canvis



Recursos útils

Podeu trobar el contingut d'aquesta presentació i altra informació rellevant sobre ciberseguretat al nostre web:

- **https://www.bsa.cat/ca/la-seguretat-es-cosa-de-tots**
  - *Accés treballadors → Procés de TransFORMAció Digital → Ciberseguretat*
- Canals de contacte:
  - Per **dubtes, peticions o consultes** de ciberseguretat → Utilitzeu GLPI
  - Per **incidents o problemes de ciberseguretat** que requereixin acció urgent:
    → Utilitzeu la bústia **ciberseguretat@bsa.cat**, o bé
    → Contacteu la responsable de ciberseguretat (Telf. 90177)