



Cruz Roja



Riesgos con las TIC

**Para más información
por favor contacta con:**

Intervención Social / Otros Colectivos Desfavorecidos

Ana Belén García Cazalla: anabelen.garciac@cruzroja.es

Alvaro Barco Barrios: Voluntario digital



Contenidos

Ciberadicción. Internet, Redes Sociales y Videojuegos	3
Nomofobia. Tiempo de uso dispositivo móvil.	6
Aislamiento digital	8
Ciberacoso	9
Ciberseguridad. Ingeniería Social.	15
Huella digital	24

Ciberadicción

La ciberadicción es una patología que se caracteriza por un uso obsesivo y adictivo de las nuevas tecnologías durante el día a día de la persona.

Señales que revelan una adicción

- Aislamiento social
- Problemas de conducta
- Irascibilidad/agresividad
- Fracaso escolar
- Problemas de sueño.
- Abandono de las actividades de ocio.
- Deterioro de las relaciones familiares y sociales.
- Empeoramiento del rendimiento académico.
- Enfados excesivos cuando falla la conexión a Internet o la navegación es muy lenta



Ciberadicción

La ciberadicción es una patología que se caracteriza por un uso obsesivo y adictivo de las nuevas tecnologías durante el día a día de la persona.

Clases de adicción:

- Adicción a los videojuegos. Aunque también se presenta en otras edades, es una de las más frecuentes entre la gente joven.
- Adicción al cibersexo. Puede dar lugar a una práctica compulsiva del sexting. Y este, a su vez, tener consecuencias como la sextorsión.
- Adicción a la obtención o inversión de bienes en Internet. Hablamos de compras en línea, juegos de azar, comercio de acciones, subastas online, uso e inversión de criptomonedas, etc.
- Adicción a las relaciones cibernéticas. Sobre todo, a través de plataformas, como redes sociales y chats, en las que es posible interactuar constantemente.
- Adicción a la búsqueda de información. La posibilidad de encontrar tanta información en la Red de manera sencilla también provoca un uso intensivo de Internet.



Ciberadicción

La ciberadicción es una patología que se caracteriza por un uso obsesivo y adictivo de las nuevas tecnologías durante el día a día de la persona.

Consejos:

- Usar los dispositivos en un horario adecuado y establecer un tiempo máximo de conexión a Internet.
- Moderar el uso de videojuegos en la Red y dedicar el tiempo de conexión a tareas más interesantes.
- Reforzar la seguridad de los dispositivos para evitar ciberamenazas
- Buscar alternativas al uso de Internet en el tiempo libre.
- Respetar las horas de sueño y comida.
- Dedicar más tiempo a las relaciones personales presenciales.
- Por último, si nos advierten o somos conscientes de nuestra condición de ciberadictos, se debe buscar ayuda profesional.



Nomofobia

Miedo irracional a estar sin móvil

Afecta al 53% de los usuarios. 58% Hombres frente al 48% Mujeres

Síntomas: Agresividad, dificultad para concentrarse e inestabilidad emocional.

Soluciones: Autocontrol

- Apaga el terminal por la noche
- Deja tu teléfono en otra habitación
- Disminuye progresivamente el tiempo de uso
- Elimina aplicaciones innecesarias
- Pequeñas salidas sin teléfono
- Limita tus horarios
- Busca ayuda profesional



Tiempo de uso dispositivo móvil

Es algo al que nos referimos como **Bienestar o Salud digital**



Fuente: [Cómo saber cuantas horas pasas usando tu móvil Android](#)

Tiempo de uso dispositivo móvil

Aplicaciones de tiempo de uso

 Google Bienestar digital 1.6.521068621.495938 Racionaliza el uso de tu smartphone ★★★★★ GRATIS 25/04/2023 15,7 MB Android Inglés
 ActionDash 9.0.6 Controla cuánto tiempo usas el móvil y en qué aplicaciones ★★★★★ GRATIS 03/01/2023 12,8 MB Android Español
 Forest 4.66.1 Mejora tus hábitos de concentración y atención ★★★★★ GRATIS 30/12/2022 163,3 MB Android Español

 StayFree 10.4.0 Controla tu adicción al móvil ★★★★★ GRATIS 14/11/2022 22,6 MB Android Español
 Star Cleaner & Booster 2.3.8 Optimiza tu Android con un toque ★★★★★ GRATIS 19/08/2022 30,7 MB Android Español
 Focus Plant 2.8.3 Olvídate del móvil y haz crecer plantas mágicas ★★★★★ GRATIS 08/06/2022 77 MB Android Inglés

 Mind Leak 1.2.0.4 Mira qué cara pones mientras procrastinas ★★★★★ GRATIS 07/06/2022 8,3 MB Android Español
 WaLog 1.2.2 Controla el tiempo de uso que tus hijos hacen del móvil ★★★★★ GRATIS 07/06/2022 26,4 MB Android Español
 Screen Time 3.1.4 Controla el tiempo de uso de tu smartphone ★★★★★ GRATIS 18/05/2022 5,6 MB Android Español
 OFFTIME 4.1.4 Cómo evitar distracciones mientras trabajas o te relajas ★★★★★ GRATIS 28/04/2022 20,4 MB Android Inglés

Aislamiento digital y redes sociales

¿Qué es lo más importante para vosotros? Amigos

Para muchos de vosotros es tener conexión a internet y un móvil

- Los chicos y las chicas usan sus dispositivos con fines sociales, para estar conectados con sus iguales.
- Uso en exceso de las redes sociales puede provocar que las personas entren en aislamiento social.
- Se sienten mal si llegan a ver publicaciones de amigos que muestren situaciones que ellos no se pueden permitir.
- La atracción de las RRSS es comparable con los casinos, en este caso las reacciones a las publicaciones, estados, vistas y 'likes' son los premios.
- RRSS provocan que respondas a la interacción social gracias a la estrategia invertida, cuando se sabe que algún usuario ha leído un mensaje se siente ansiedad por recibir la respuesta o por responder.



Ciberacoso

Afecta al 84% de los usuarios en España

Riesgos propios o derivados del entorno digital:

- **Ciberacoso o cyberbullying**, acoso entre iguales a través de medios digitales, que puede continuar o no en el entorno analógico, o derivar de él.
- **Grooming y otras citas** con personas extrañas, solo contactadas por RRSS.
- **Sexting y extorsión**, compartir contenido audiovisual de carácter sexual propio o de otra persona que no consiente su captura.
- **Doxing** y Suplantación de la identidad.
- Conflictos derivados de retos virales.
- **Sharenting**, práctica en expansión de los padres y madres de compartir fotos, vídeos u otra información de sus hijos en redes sociales.

Ciberacoso

Afecta al 84% de los usuarios en España

Riesgos propios o derivados del entorno digital:

- **Discurso de odio**, publicación de comentarios a través de Internet para atacar a colectivos determinados.
- **Cibercontrol**, control entre parejas jóvenes a través de medios digitales. Y aspectos más relacionados con adicciones o trastornos como:
- **Phubbing**, cuando una persona ignora a otra y se abstrae del entorno que le rodea al estar más pendiente de su teléfono móvil que de sus acompañantes humanos.
- **Ludopatía**, patología que consiste en una alteración progresiva del comportamiento por la que el individuo experimenta una necesidad incontrolable de jugar, por encima de cualquier consecuencia negativa. (Poker, apuestas, bitcoin....)
- **Vamping**, uso de aparatos electrónicos antes de dormir con la consecuente reducción de las horas de sueño, es un fenómeno en auge, sobre todo en adolescentes.

Línea de Ayuda en Ciberseguridad 017. Gratuito.



- El teléfono seguirá siendo accesible desde toda España, y podremos llamar entre las 9:00 y las 21:00 en cualquier día del año (incluyendo sábado, domingo y festivos) sobre cualquier duda relacionada con ciberseguridad, privacidad, confianza digital, uso seguro y responsable de Internet y de la tecnología.
- Además, cuenta con alternativas como los canales de chat de WhatsApp y Telegram que permiten un contacto más cercano con los usuarios, proporcionando mayores prestaciones de accesibilidad a aquellos ciudadanos con dificultades en la comunicación, como puede ser el colectivo de personas sordas.

[WhatsApp 900 116 117](https://www.whatsapp.com/channel/0029va8116117) – [Telegram @INCIBE017](https://t.me/INCIBE017)

Qué delitos puedes denunciar

Podrán recibir atención relacionada con diferentes delitos dependiendo de si son personas, empresas o menores.

- **Empresas:** atención sobre organización de la ciberseguridad en la empresa y principales problemas relacionados con la protección de datos y otros incidentes de seguridad como el ransomware.
- **Ciudadanos:** podrás recibir atención y asesoramiento relacionado con la protección de dispositivos, conexiones, privacidad, tipos de fraudes, virus y todo tipo de programas maliciosos.
- **Internet Segura for Kids (IS4K):** aquí los padres y educadores podrán realizar consultas relacionadas con el uso de Internet y las tecnologías por menores y adolescentes. Además, recibirán asesoramiento psicosocial, técnico y legal sobre situaciones de riesgo y conflictos de los menores en Internet como el ciberacoso, las comunidades peligrosas o el control parental y la privacidad. Además el ciberacoso: sexting, grooming, o ciber acoso escolar, etc.

¿Qué consecuencias tiene el ciberacoso?

Cuando el acoso ocurre en línea, la víctima siente como si la estuvieran atacando en todas partes, hasta en su propia casa. Las consecuencias:

- **Mentalmente.** Se siente preocupada, avergonzada, estúpida y hasta asustada o enfadada.
- **Emocionalmente.** Se siente avergonzada y pierde interés en lo que le gusta.
- **Físicamente.** Se siente cansada (pierde el sueño) o sufre dolores de estómago y de cabeza.

Soluciones

- Piensa dos veces antes de publicar o compartir algo en plataformas digitales.
- No des detalles personales como tu dirección, tu número telefónico o el nombre de tu escuela.



CONSEJOS PARA HACER UN BUEN USO DE REDES SOCIALES

Andalucía se mueve con Europa

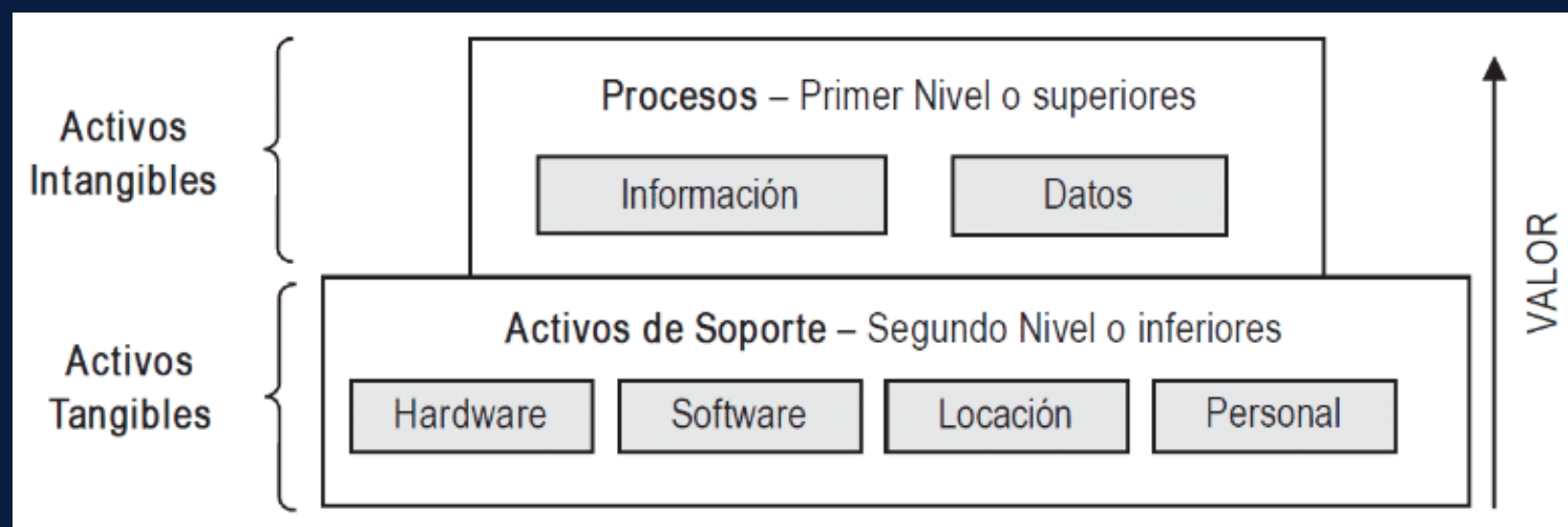
- 1 PROTEGE TUS DATOS Y CONFIGURA LA PRIVACIDAD EN TUS REDES**
Configura la privacidad y decide quien puede ver tus publicaciones.
- 2 LAS CONTRASEÑAS SON PRIVADAS, NO LAS FACILITES A NADIE**
Crea contraseñas robustas y no las compartas con nadie. Piensa que pueden hacerse pasar por ti.
- 3 NO ACEPTES SOLICITUDES DE PERSONAS QUE NO CONOCES**
Desconoces quién hay realmente detrás de ese perfil y sus intenciones. Por ello acepta sólo peticiones de amistad de personas que conoces personalmente.
- 4 NO QUEDES CON PERSONAS QUE SÓLO CONOCES DE REDES SOCIALES**
No es seguro quedar con personas que no conoces personalmente, pero si lo haces acude siempre acompañado/a de otra persona.
- 5 EVITA PUBLICAR INFORMACIÓN PERSONAL NI FAMILIAR**
No des información de donde vives ni con quien estás, cuida tu seguridad.
- 6 PIENSA DOS VECES LA IMAGEN QUE VAS A COMPARTIR**
Cada vez que publicamos algo en una red social perdemos el control sobre ese contenido. Una buena forma de decidir si es íntimo, es pensar si te importaría que lo vieran tus familiares.

Ingeniería Social

Que es y cómo protegernos

Basa su comportamiento en una premisa básica: es más fácil manejar a las personas que a las máquinas. Para llevar a cabo este tipo de ataque se utilizan técnicas de manipulación psicológica y habilidades sociales con el objetivo de manipular, engañar, influenciar y conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente.

Fuente: Incibe



La IS puede ser utilizada con diferentes fines:

- * Ingeniería social con intenciones maliciosas o económicas
- * Ingeniería social con buenas intenciones
- * Ingeniería social con intenciones personales

Así mismo existen dos tipos de IS:

- Ingeniería Social Presencial
- Ingeniería Social No Presencial

Cómo se comunican los ciberdelincuentes

- * Ingeniería Social de Comunicación Directa
 - * Bidireccional y Unidireccional
- * Ingeniería Social de Comunicación Indirecta



Ingeniería Social

Que técnicas utilizan:

Los atacantes de ingeniería social pueden hacerse pasar por personas de confianza, como técnicos de soporte, empleados de una empresa asociada o de servicios, para solicitar información confidencial o acceso a sistemas. También pueden utilizar tácticas de persuasión, como la creación de una falsa sensación de urgencia o la creación de un escenario amenazante para presionar a las personas a realizar acciones no deseadas.

1. **Respeto a la autoridad.**
2. **Voluntad de ayudar.**
3. **Temor a perder un servicio.**
4. **Gratis.**

Fuente: Universidad de las Américas Puebla



Entornos Digitales Seguros

Como prevenirnos y evitar caer

Las mejores prácticas para que un usuario implemente una mejora de su seguridad en línea son:

1. Actualiza tu software
2. Utiliza contraseñas fuertes
3. Desconfía de los correos electrónicos sospechosos
4. Utiliza software de seguridad
5. Mantén la privacidad en línea
6. Haz copias de seguridad de tus datos:



Avast Security

NOVEDAD

Las filtraciones de datos son más peligrosas de lo que piensa

Cada año se producen miles de filtraciones de datos. Si sus datos se filtran, los hackers pueden acceder a sus cuentas y utilizar su identidad en su propio beneficio.

- 1 **Sus datos bancarios** y su información confidencial pueden quedar expuestos.
- 1 **Sus credenciales de inicio de sesión**, correos electrónicos privados e incluso su identidad se pueden robar.
- 1 **Sin alertas instantáneas**, podría darse cuenta demasiado tarde, lo que dañaría sus cuentas y su reputación.

CONTINUAR






Entornos Digitales Seguros

Como prevenirnos y evitar caer

HTTPS: Es un protocolo de seguridad de internet que se utiliza para proteger los datos en tránsito entre un navegador y un sitio web.

Para comprobar la seguridad de un sitio, a la izquierda de la dirección web, consulta el símbolo de estado de seguridad:

-  Es seguro
-  Información o No es seguro
-  No es seguro o Es peligroso

2o factor de autenticación en todas tus plataformas: el primero factor de autenticación es usuario/contraseña, un segundo elemento de identificación, de la terna lo que soy, lo que sé o lo que tengo, normalmente por otro medio alternativo para acceder.



Fuente:

<https://conectate.educaciontuc.gov.ar/manual-de-prevencion-en-entornos-digitales-conductas-de-riesgo-y-ciberdelitos-en-internet-ciberbullying-sexting-grooming-y-trata-de-personas/>

Seguridad en el correo electrónico

(herramientas para hacer seguro un correo electrónico).

Son las medidas que se toman para proteger la información personal y confidencial que se transmite a través de correo electrónico. Esto incluye proteger la privacidad de las comunicaciones, asegurarse de que los mensajes se entreguen correctamente, evitar que los mensajes sean interceptados o leídos por terceros no autorizados, y prevenir el acceso no autorizado a la cuenta de correo electrónico en sí misma.

Algunas de las medidas de seguridad que se utilizan en los correos electrónicos incluyen la encriptación, la autenticación de dos factores, la verificación de la dirección del remitente, la utilización de contraseñas seguras y la prevención del phishing.



Tipos de amenazas:

- **Filtración de datos**
- **Malware**
- **Spam**
- **Suplantación**
- **Phishing**



Cuidémonos de los Phishing.

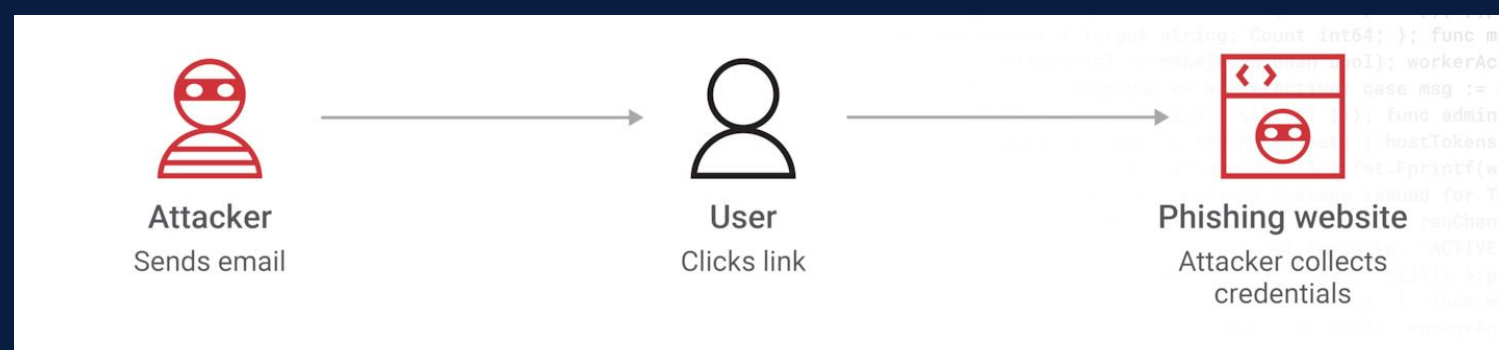
Es importante tomar medidas para protegernos contra el phishing y evitar que los ciberdelincuentes roben nuestra información personal. Siempre es mejor ser cauteloso y sospechar de cualquier mensaje o correo electrónico que parezca sospechoso o no solicitado.

Algunos datos:

- La ingeniería social es responsable del 98% de todos los ataques de phishing
- Más del 70% de las filtraciones de datos empiezan por phishing o ingeniería social.
- Google ha registrado más de 2 millones de websites de phishing.



Fuente: <https://www.bbva.com/es/innovacion/phishing-y-smishing-que-son-y-como-evitarlos/>



Cuidémonos de los Phishing.

Cómo evitar la ingeniería social y el Phishing

La sensación de urgencia del mensaje pilla desprevenidas a muchas víctimas, pero los usuarios bien formados pueden seguir los pasos necesarios para saber cómo evitar la ingeniería social y no resultar víctimas, siguiendo algunas reglas.

Investigar antes de responder: Si la estafa es común, entonces podrá encontrar en internet otras personas hablando acerca del método de ingeniería social.

No interactuar con una página web de un enlace: Si el remitente afirma provenir de un negocio oficial, no haga clic en el enlace para autenticar. En lugar de eso, escriba el dominio oficial en el navegador.

Tenga cuidado con comportamientos sospechosos por parte de amigos: Los atacantes usan cuentas de correo electrónico hackeadas para engañar a los usuarios.

No descargue archivos: Si un correo electrónico le pide urgentemente que descargue un archivo, ignore la solicitud o pida ayuda para asegurarse de que la solicitud sea legítima.



Cuidémonos de los Phishing.

ND NOTIFICACION DAVIPLATA
urbano1474@hotmail.com

To You alva [redacted]
Saturday, March 11, 14:58

[DAVIPLATA.W.W.W.COM](#)
Estimado(a)
a [redacted]

Hemos recibido una solicitud de Cambio de Numero celular al 321***47 el dia de hoy 11/03/2023

recientemente hemos encontrado actividad inusual con su daviplata, por lo que bajo el Regimen 99713 hemos bloqueado su cuenta de forma temporal.

Si no has sido tu quien incumplio con la politica de uso de Daviplata | Davivienda o piensas que fue un error, visita nuestro Portal de Ayuda Daviplata.

Ingresar Aqui =====> [shampinplatinplata.0hi.me/](#)

1. Ingresar a Nuestro Portal

[DAVIPLATA.W.W.W.COM](#)
Estimado(a)
a [redacted]


Hemos recibido una solicitud de Cambio de Numero celular al 321***47 el dia de hoy 11/03/2023

recientemente hemos encontrado actividad inusual con su daviplata, por lo que bajo el Regimen 99713 hemos bloqueado su cuenta de forma temporal.

Si no has sido tu quien incumplio con la politica de uso de Daviplata | Davivienda o piensas que fue un error, visita nuestro Portal de Ayuda Daviplata.

Ingresar Aqui =====> [shampinplatinplata.0hi.me/](#)


1. Ingresar a Nuestro Portal
2. Valida el proceso de verificacion
3. IngresarCodigo 6 Digitos Via SMS



Estimado cliente,

Su paquete está esperando la entrega. Confirme el pago (2,99EUR) en el siguiente enlace, la verificación en línea debe hacerse en los próximos 14 días antes de que caduque.

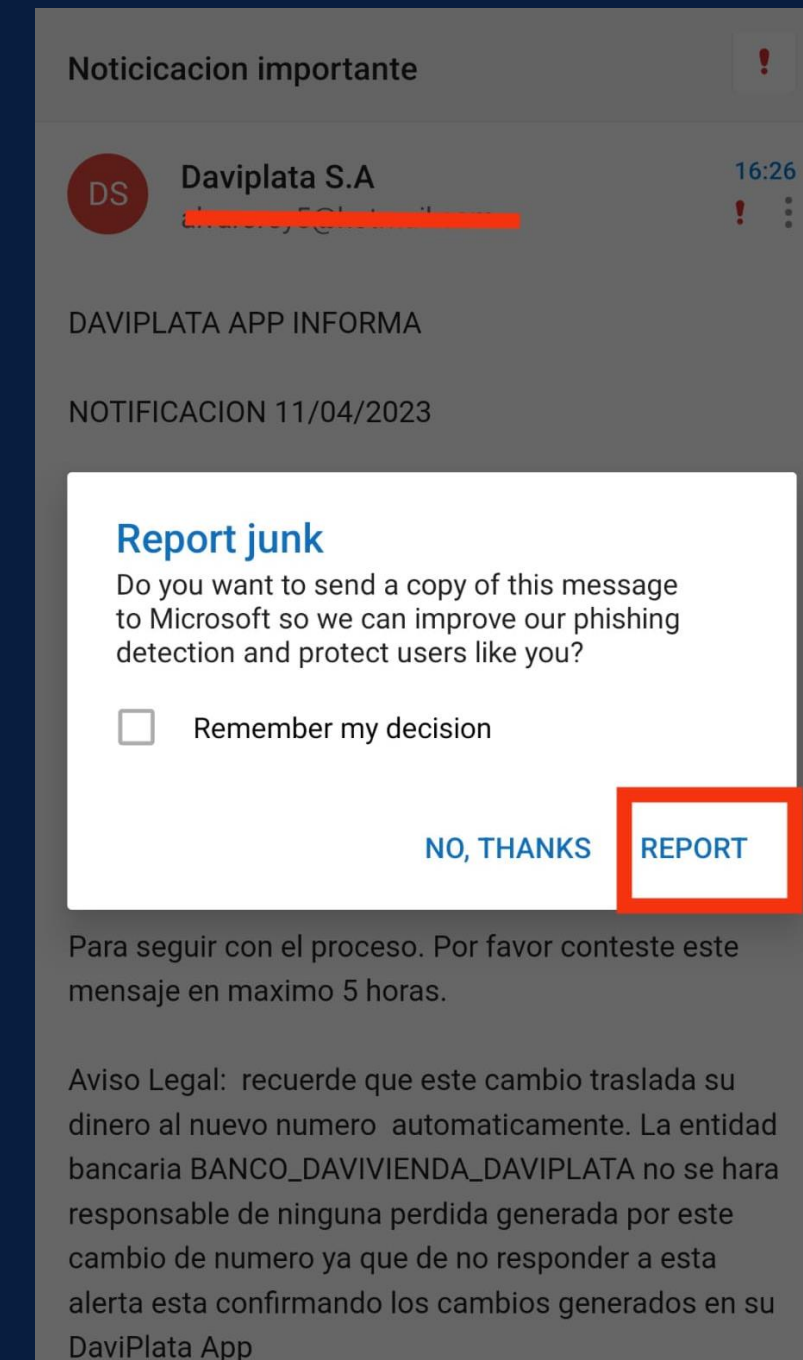
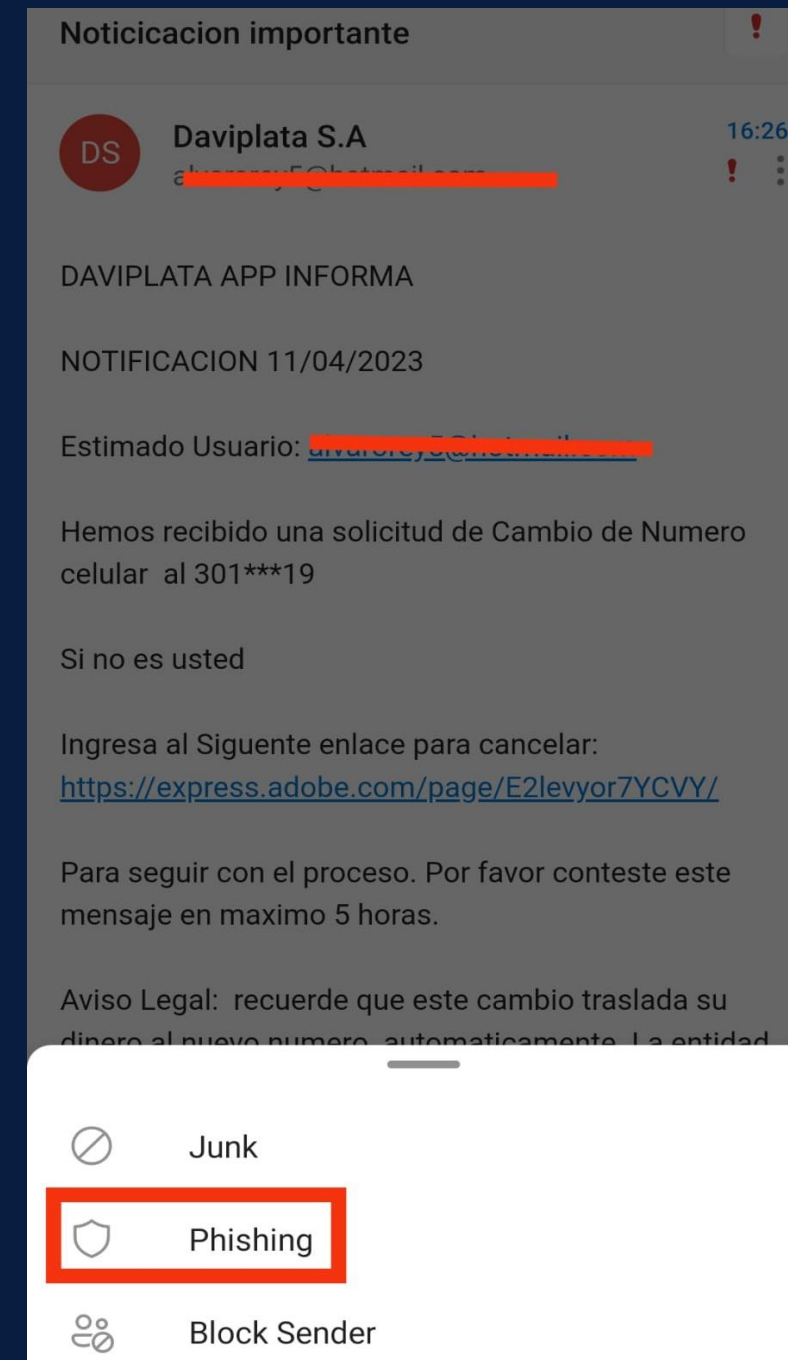
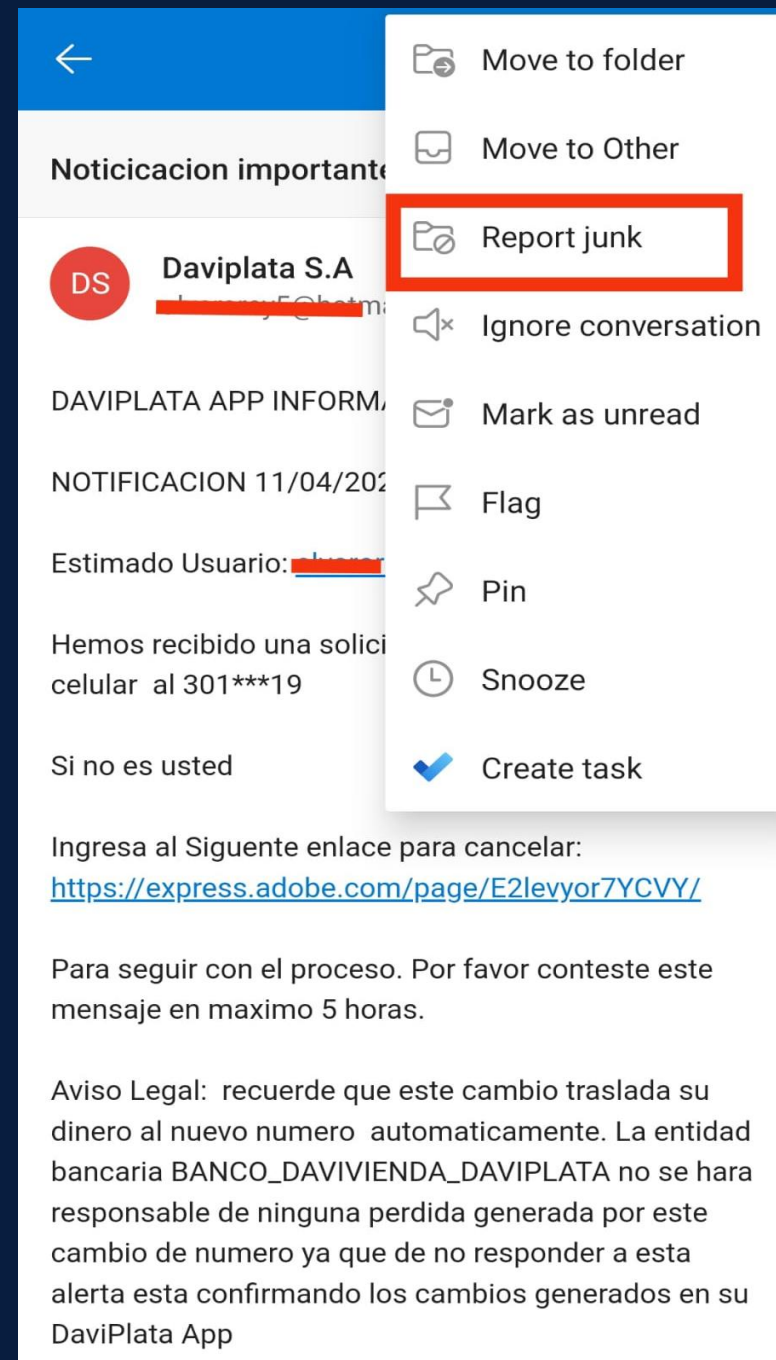
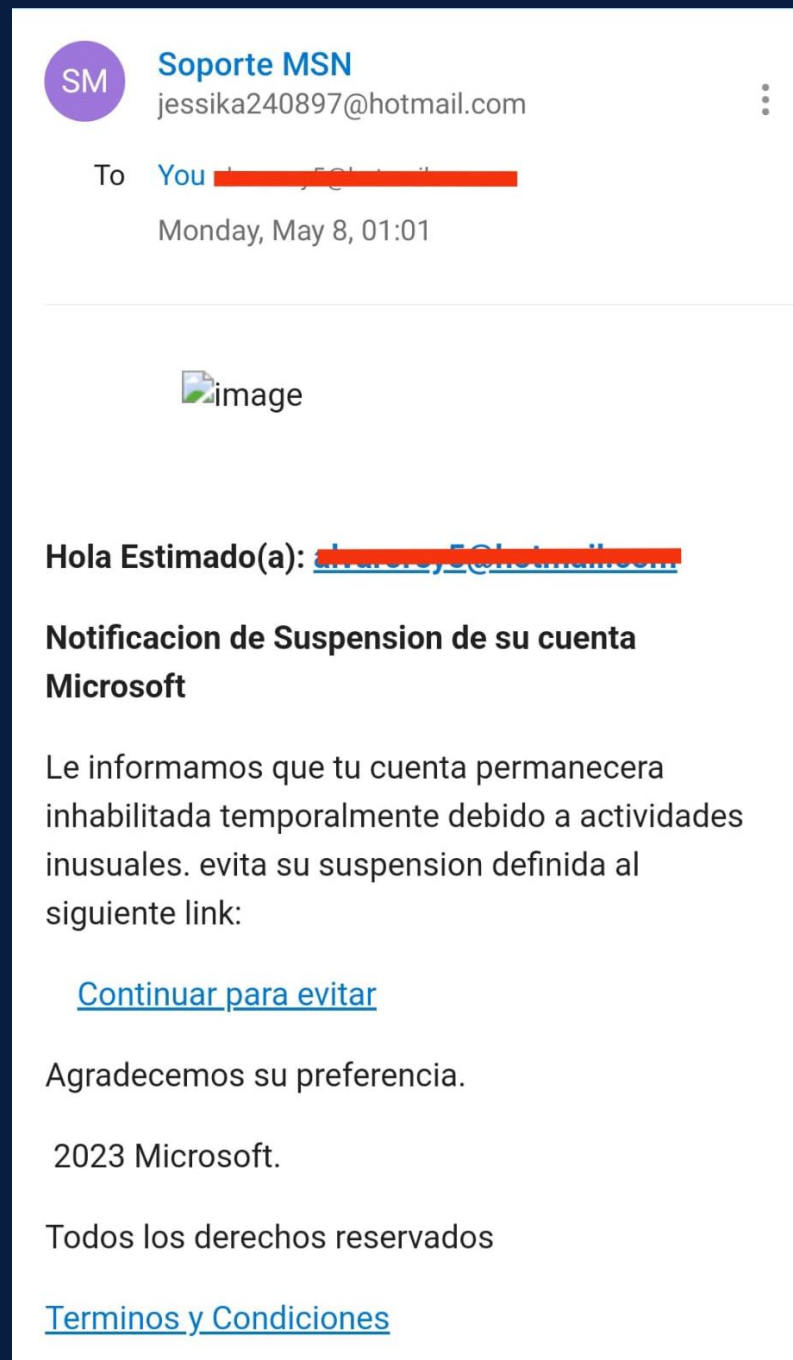
[Haga clic aquí](#)



13:38

Apreciado cliente:
Su paquete no pudo entregarse el [1/11](#) porque no se pagaron las tasas aduaneras (1€).
Encontrara mas datos aqui:
<http://3cm.top/LexJ>

Cuidémonos de los Phishing.



Huella Digital en Internet.

Que es y cómo protegerla

Es la información única y los rastros digitales dejados por una persona en internet. Estos rastros pueden incluir datos como publicaciones en redes sociales, comentarios en blogs, compras en línea, actividad de navegación, correos electrónicos enviados y recibidos, registros en sitios web.

Cada interacción que tienes en internet deja una huella digital, y con el crecimiento de las plataformas en línea y la recopilación de datos, tu huella digital puede ser bastante extensa



Tu información de huella recopilada en internet puede ser utilizada por empresas, anunciantes u otros terceros para rastrear tus actividades, enviarte publicidad personalizada o incluso para fines más malintencionados, como el robo de identidad.






Huella Digital en Internet.

Cómo protegerla






- Configuración de privacidad: Revisar y ajustar la configuración de privacidad en las redes sociales y otras plataformas en línea es fundamental.
- Uso de navegación privada: Utilizar modos de navegación privada o utilizar una VPN (red privada virtual).
- Gestión de cookies: Configurar el navegador para que bloquee o limite las cookies puede reducir el seguimiento de tus actividades en línea.
- Uso de alias y pseudónimos: Considera utilizar alias o pseudónimos en línea en lugar de tu nombre real para ciertas actividades.
- Cuidado con la información personal: Piensa dos veces antes de compartir información personal en línea, como tu dirección, número de teléfono o detalles bancarios.
- Contraseñas seguras y autenticación de dos factores: Utiliza contraseñas fuertes y únicas para tus cuentas en línea, y habilita la autenticación de dos factores siempre que sea posible.
- Educación sobre seguridad en línea: Mantente informado sobre las prácticas de seguridad en línea, como el phishing, el malware y el robo de identidad.
- Limitar la exposición en redes sociales: Considera reducir la cantidad de información personal que compartes en redes sociales y evita publicar detalles sobre tu ubicación en tiempo real.

INTERNET SEGURA 1

¿Qué es una página web falsa?


-  Una página que intenta engañarnos, normalmente para robar datos. 
-  Un sitio al que nos podemos conectar para tener charlas virtuales.
-  La descarga de una página web.
-  Los datos que guarda nuestro ordenador cuando accedemos a una web.

¿En qué puedes fijarte para detectar un engaño por correo?


-  Revisando quién me envía el mensaje.
-  Revisando el texto del mensaje en busca de errores.
-  Acudiendo directamente a la página web oficial sin pinchar en el correo.
-  Todas las respuestas son correctas. 

INTERNET SEGURA 1

3 - Quiz
¿Cómo podemos detectar una dirección web (URL) fraudulenta?

- Comparto la dirección a alguien de clase.
- Usando comprobadores de enlaces. 
- Haciendo clic para ver dónde me lleva.
- No se puede detectar.

4 - Quiz
¿Cómo podrías evitar que una app descargada infectara tu dispositivo?


- Pinchando en enlaces que anuncian aplicaciones gratis.
- Usando tiendas de apps gratuitas.
- Descargando de sitios oficiales, comprobando la información y las opiniones 
- No se puede hacer nada.

5 - Quiz
¿Dónde puedes acudir si tu familia y tú necesitáis ayuda?

- Pregunto a mis padres, u otro adulto de confianza.
- Llamo al 017 (INCIBE), Tu Ayuda en Ciberseguridad.
- Pregunto a mis profesores.
- Todas las respuestas son correctas. 


INTERNET SEGURA 2

¿Qué acción ayuda a que no adivinen tu patrón de desbloqueo?

- Limpiar la pantalla. 
- Bajar el volumen.
- Bajar el brillo de la pantalla.
- Activar el modo avión.


2 - Quiz

¿Qué aplicación puede ayudarte a recordar contraseñas?

- La calculadora.
- La agenda de contactos.
- Un gestor de contraseñas. 
- Una red social.


3 - Quiz

¿Qué harías para evitar que cualquiera pueda descargarse una de tus fotos?


- Configuro mi perfil en modo privado.
- Limito quién puede ver mis publicaciones.
- No acepto solicitudes de amistad de desconocidos.
- Todas son correctas. 

INTERNET SEGURA 2


4 - Quiz
¿Cómo puedes añadir un extra de seguridad a tus cuentas de Internet?

- Usando una cuenta de recuperación confiable como la de mis padres.
- Creando contraseñas largas y difíciles de adivinar.
- Todas son correctas. 
- Usando doble factor de autenticación.


5 - Quiz
¿Qué es una cuenta/correo de recuperación?

- Una cuenta cuya contraseña comparto con mis amigos.
- Una alternativa con la que poder recuperar la contraseña de otro servicio. 
- Una cuenta en la que utilizo la misma contraseña.
- Todas las anteriores son correctas.

6 - Quiz
¿Qué es el doble factor de autenticación?

- El código de recuperación de contraseña.
- Una contraseña robusta.
- Un tipo de ciberataque.
- Un código adicional a la contraseña, necesario para acceder a mis cuentas. 

7 - Quiz
¿Dónde puedes acudir si tu familia o tú necesitáis ayuda?

- Pregunto a mis padres, u otro adulto de confianza.
- Llamo al 017 (INCIBE), Tu Ayuda en Ciberseguridad.
- Pregunto a mis profesores.
- Todas las respuestas son correctas. 



¡GRACIAS!



voldigital@cruzroja.es

cruzroja.es