Unión de Radioaficionados Españoles.

Sección de VALLADOLID 2021

Consejos básicos de Ciberseguridad.

URE Valladolid 2021

Foto de tumisu https://pixabay.com/es

- Pandemia.
- Rápida expansión de Internet, nadie se puede quedar atrás.

- Avances tecnológicos.
- Aumento de la capacidad de la redes de comunicación.
- Aumento de la capacidad de procesamiento de datos.

- *Oportunidad para TODOS*.

(Buenos y no tan buenos)

Internet …..

- Portales con contenidos de una gran calidad.
- Un lugar de interacción a nivel mundial.
- Fuente inagotable de información, y des-información.
- “ Lo pone en Internet”,es palabra de Dios”, un ejemplo : “la Tierra es plana”.
- Es un lugar de oportunidades; laborales, comerciales, sociales.
- A día de hoy , el nuevo campo de batalla para los países (China, EE.UU, Rusia, India, Pakistán, Irak, Israel), creación de Cyber ejércitos, ataques a estructuras críticas y/o sectores estratégicos.
- Plataforma ideal para el espionaje industrial.
- Si dispones de dinero , puedes comprar lo que quieras (DarkWeb).

Internet en el cuarto de radio.

- Búsqueda de información, técnica, manuales, equipos, etc.
- Blogs, grupos de trabajo, expediciones, concursos,manejo estaciones remotas.
- Información en tiempo real , propagación, cluster web, logs en linea.
- Facilita el desarrollo personal y técnico (Proyectos,”cacharreo”).
- Afianza nuestra identidad como colectivo.
- Es una parte fundamental y necesaria del cuarto de radio.

Foto de Wallace Chuck en Pexels

¿*Qué podemos hacer ante las amenazas*?

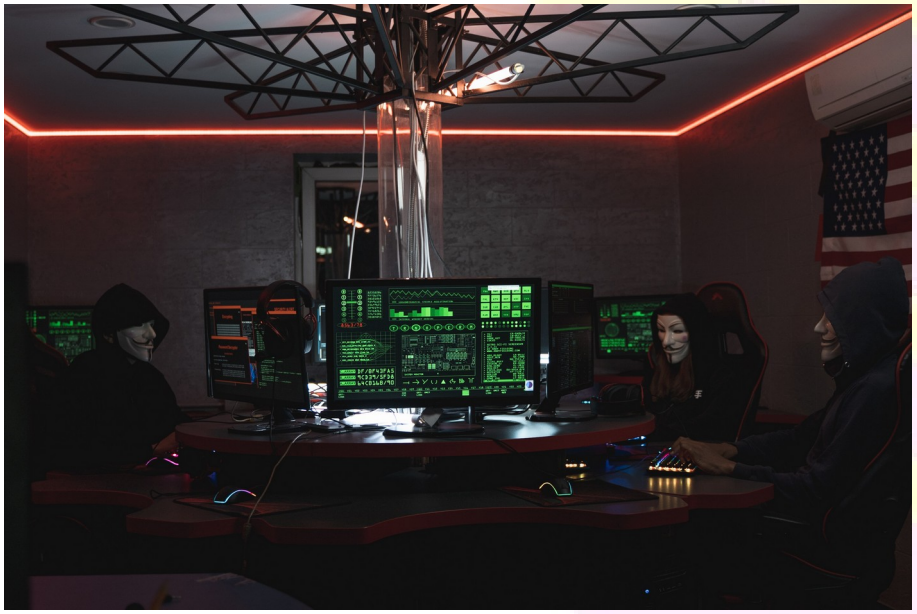


Foto de Tima Miroshnichenko en Pexels

- No entrar en pánico.
- Ser conscientes de los riesgos que existen en la utilización de las TI (Internet).
- Asumir: “En cualquier momento,podemos ser víctima de un ciberataque.”
- Aplicar medidas,para mitigar o reducir las consecuencias de un ataque.
- NO podemos garantizar la seguridad al 100 % .La ley del mínimo esfuerzo, siempre habrá un equipo/ dispositivo más fácil de atacar.

Tipos de amenazas.

https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html)

Malware

Malware es un término que se usa para describir el *software malicioso*, que incluye spyware, ransomware, virus y gusanos. El malware infringe las redes mediante una vulnerabilidad, usualmente cuando un usuario *hace clic en un enlace* peligroso o en un *archivo adjunto de correo electrónico* que, luego, instala un software. Una vez dentro del sistema, el malware puede hacer lo siguiente:

- Bloquear el acceso a los componentes clave de la red (ransomware).
- Instalar malware o software dañino adicional.
- Obtener información furtivamente mediante la transmisión de datos del disco duro (spyware).
- Alterar ciertos componentes y hacer que el equipo sea inoperable.

Tipos de amenazas.

https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html)

Suplantación de identidad (phishing)

La suplantación de identidad (phishing) es la práctica de *enviar comunicaciones fraudulentas que parecen provenir de fuentes confiables*, habitualmente a través del correo electrónico. El *objetivo es robar datos sensibles, como información de inicio de sesión y tarjetas de crédito*, o instalar malware en la máquina de la víctima. La suplantación de identidad (phishing) es una ciberamenaza cada vez más común.

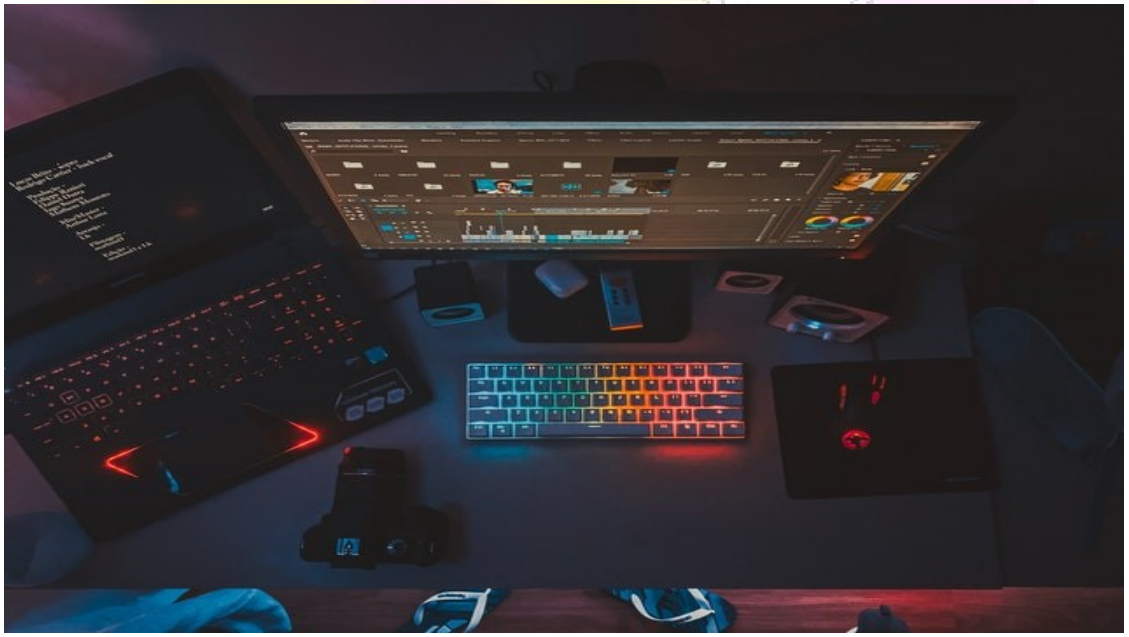


Foto de OTAVIO FONSECA en Pexels

La lista es mucho más amplia , para saber más de los tipos de amenazas y como se realizan , se encuentra en portales de Internet información muy interesante con un lenguaje claro , sin tecnicismos que exponen las amenazas en la red:

- https://www.osi.es/es/guia-ciberataques
- https://www.is4k.es/blog/alfabetizacion-mediatica-para-proteger-los-y-las-menores-frente-los-deepfakes
- https://www.incibe.es/

Los enlaces mostrados son una visita obligada, siempre aprenderemos algo y están actualizados con las últimas técnicas utilizadas por los ciberdelincuentes (Métodos , ingeniería social).

Medidas que podemos tomar ante las amenazas en la Red.

Foto de Kevin Ku en Pexels

Medidas que podemos tomar ante las amenazas en la Red (I).

Las medidas que podemos implementar como usuarios se pueden definir de dos tipos :

- *Medidas en software y hardware*, configuraciones y actualizaciones (PC,Software, Router, Wi-Fi).
- *Pautas en Correo electrónico y navegación Web*.(Actualmente, alrededor del 95% de los ciberataques que sufren las empresas tiene su origen en el llamado «factor humano». Es decir, en los deslices que se cometen por desconocimiento o error. Fuente (Telefonica Empresas https://empresas.blogthinkbig.com/empleados-y-ciberdelincuencia/).

Tenemos que recordar, que aún aplicando medidas, *no se puede garantizar* que no seamos víctimas de un ciberataque.

Medidas que podemos tomar ante las amenazas en la Red (II).

Software:

Configuraciones y actualizaciones (PC,Software).

- Planteamiento de mínimos privilegios, trabajar como usuarios normales con mínimos privilegios, solo utilizar el rol de administrador en el caso de instalaciones de software y/o cambios de configuración.
- Actualización del software, Sistemas Operativo (SO), programas y por supuesto el antivirus. (todas las semanas aparecen vulnerabilidades en los SO, software, drivers, Firmware de los dispositivos).
- Eliminación periódica de los historiales de los navegadores , incluidos las cookies.

Tenemos que recordar, que aún aplicando medidas, *no se puede garantizar* que no seamos víctimas de un ciberataque.

Medidas que podemos tomar ante las amenazas en la Red (III).

Software:

Configuraciones y actualizaciones (PC,Software).

- Realización de copias de Seguridad (perdida de los contactos, log). Bien en nube, dispositivo Pendrive, disco duro HDD). Automático*.
- Puertos, solo los necesarios*.
- Gestión de contraseñas.
- Eliminar aplicaciones que no se usen.
- Nivel “Dios” cifrado del los ficheros.*

Tenemos que recordar, que aún aplicando medidas, *no se puede garantizar* que no seamos víctimas de un ciberataque.

Medidas que podemos tomar ante las amenazas en la Red (IV).

Router y Wi-Fi:

- Cambio de la contraseña del router para la administración del mismo.
- Actualizaciones del software del router.
- Cambio de la contraseña de la red Wi-Fi, cifrado WAP2, ocultar la red, cambio del SSID (nombre de la red wi-fi).
- Habilitar el filtro MAC para los dispositivos que se conectan a la red, en. (es como la matricula de un coche, en teoría cada mac es distinta). En algunos router se puede configurar los horarios de acceso.
- Desactivar el acceso remoto SSH.*

Tenemos que recordar, que aún aplicando medidas, *no se puede garantizar* que no seamos víctimas de un ciberataque.

Medidas que podemos tomar ante las amenazas en la Red (V).

Router y Wi-Fi:

- Deshabilitar el WPS .*
- Crear sub-red de invitados, distinta a la principal.*

* Los items marcados con * pueden necesitar un conocimiento avanzado para su configuración, al mismo tiempo pueden depender del dispositivo y la operadora de servicio.

Tenemos que recordar, que aún aplicando medidas, *no se puede garantizar* que no seamos víctimas de un ciberataque.

Medidas que podemos tomar ante las amenazas en la Red (VI).

Correo y navegación WEB:

El correo electrónico es uno de los medios más empleados para el malware y de ingeniería social. Es un vector de ataque muy común.

- En el caso que no sea marcado como spam, comprobar la dirección del remitente que tenga relación con nosotros.
- Evitar facilitar la dirección e-mail en lugares o foros que no tengan verificación de acceso o que dicha información sea accesible de forma pública.
- No acceder a los servicios de correo por medio de dispositivos ajenos o por medio de redes públicas (Wi-Fi gratis).

Tenemos que recordar, que aún aplicando medidas, *no se puede garantizar* que no seamos víctimas de un ciberataque.

Medidas que podemos tomar ante las amenazas en la Red (VII).

Correo y navegación WEB:

- Cuidado con los enlaces en los correos, a no ser que sean solicitados por nosotros , por ejemplo al solicitar nueva contraseña o al darse de alta en algún servicio o página web, portal, etc.
- Cuidado con los ficheros adjuntos, sobre todo documentos word, excel , pdf. Comprobar antes de abrir por medio de un antivirus.
- Las empresas, bancos y/o administraciones públicas ***NUNCA*** solicitan datos personales (nombre de usuario , contraseñas, comprobación de servicio).

Tenemos que recordar, que aún aplicando medidas, *no se puede garantizar* que no seamos víctimas de un ciberataque.

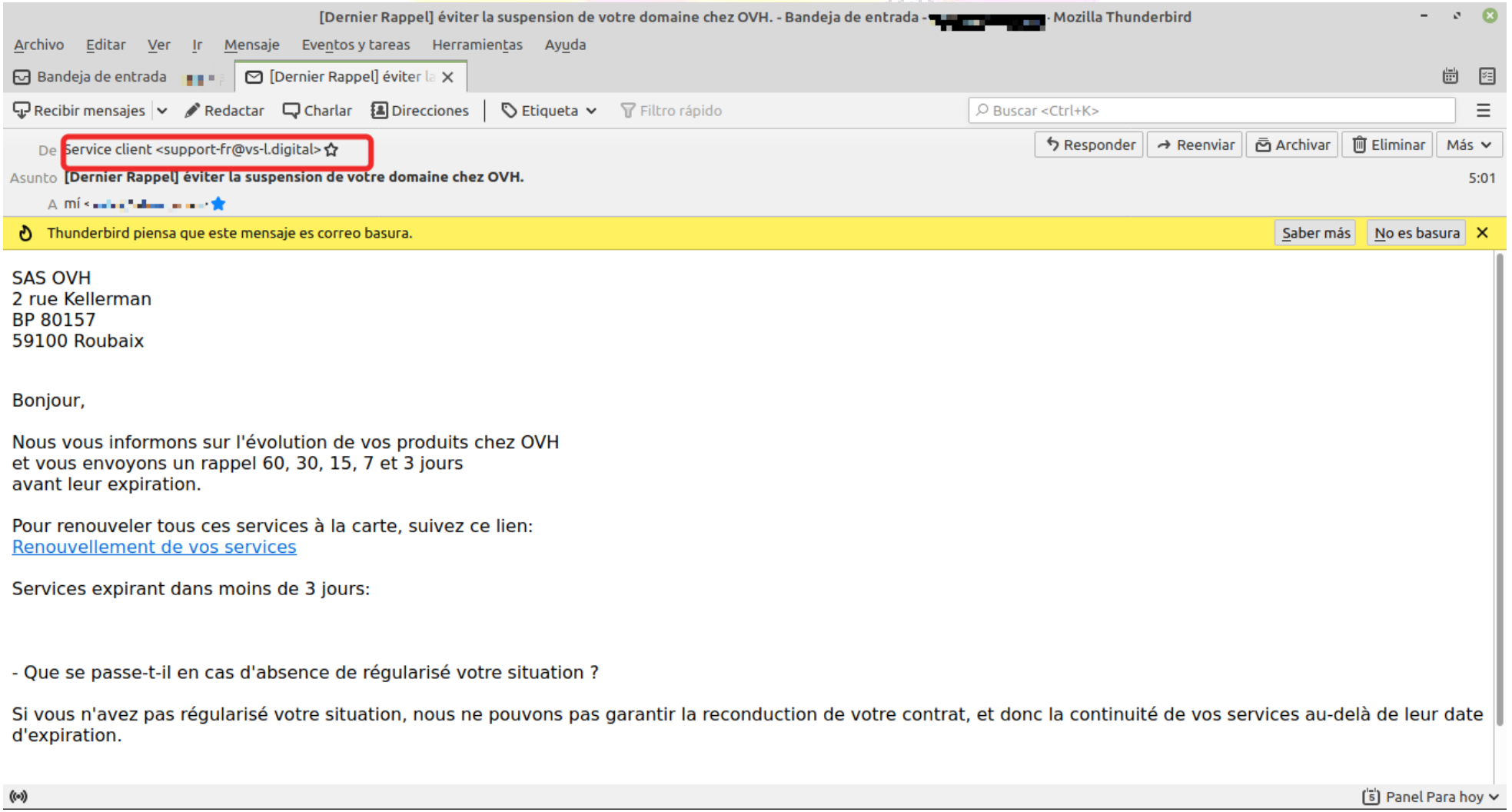
Medidas que podemos tomar ante las amenazas en la Red (VIII).

Correo y navegación WEB:

- Desconfiar de los enlaces acortados y/o códigos QR , son muy utilizados como vectores de ataque.
- Comprobar el dominio del remitente, por ejemplo : si el correo es de Vodafone no puede tener dominio hotmail, google , etc. (ejemplo).
- Añadir “puglin” a los navegadores , bloqueo de rastreadores, publicidad, ventanas emergentes solo de fuentes confiables.
- Si dudamos de la veracidad de un correo se llama a la entidad o empresa, por preguntar no pasa nada.

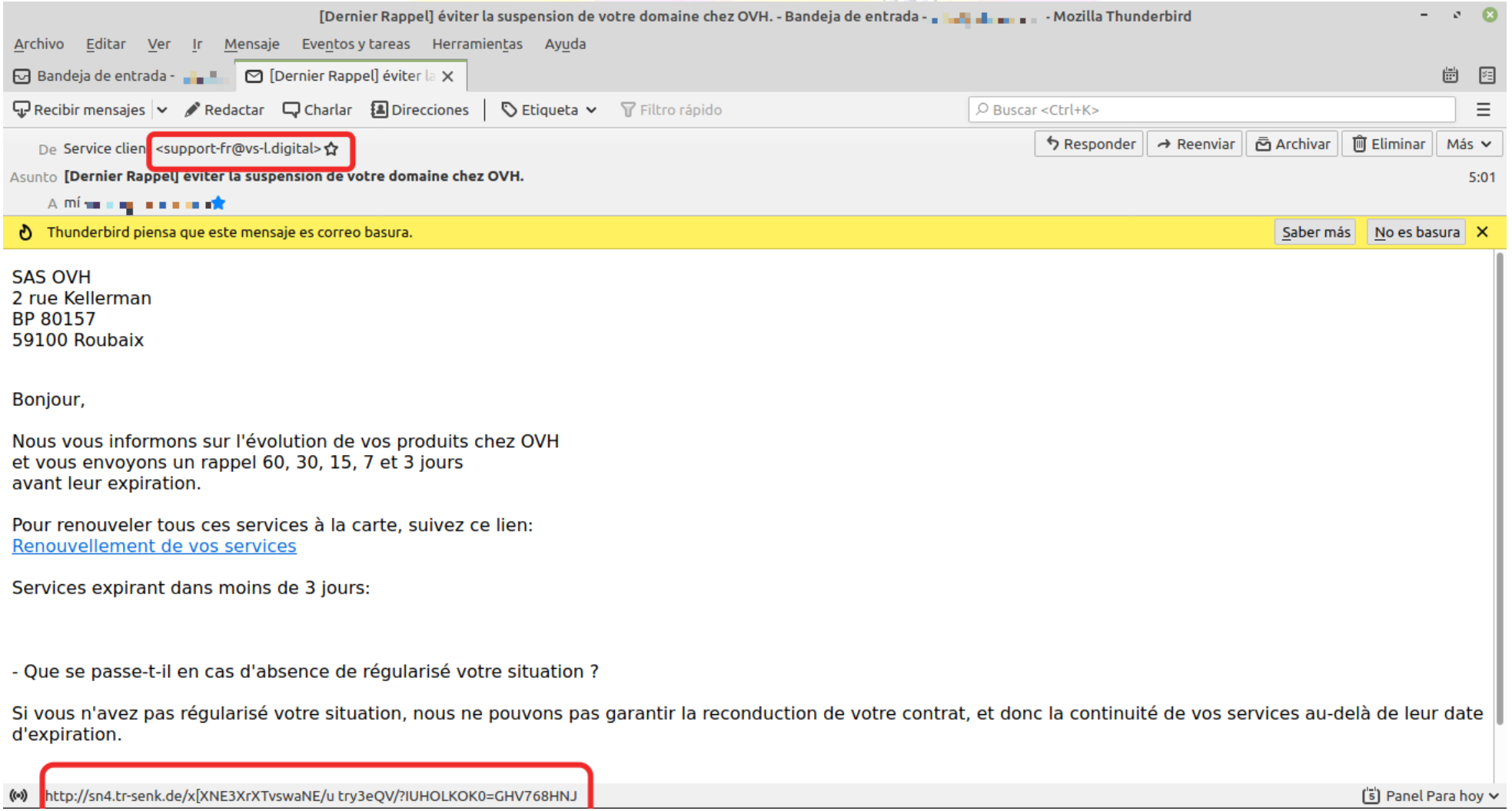
Tenemos que recordar, que aún aplicando medidas, *no se puede garantizar* que no seamos víctimas de un ciberataque.

Ejemplo de correo malicioso



URE Valladolid 2021

Ejemplo de correo malicioso



Resumen.

- Prestar atención cuando se navega por la WEB (páginas legitimas y enlaces) , y en especial con los correos electrónicos.
- Es aplicable también a los SMS y dispositivos móviles.
- Por defecto ***NO*** “pinchar” en enlaces que no podamos comprobar su origen legitimo o dudemos de su origen.
- Por defecto ***NO*** descargar ficheros que no podamos comprobar su origen legitimo o dudemos de su origen.
- Mantener los sistemas PC y dispositivos actualizados.
- Instalar antivirus y comprobar el PC con asiduidad.

Agradecimiento

Muchas gracias a todos por vuestro tiempo y la atención prestada

http://www.ea1urv.es/web/