Recomendaciones sobre seguridad

A nivel mundial se están recibiendo multitud de ataques de malware de diferentes tipos, en particular, algunas instituciones españolas han recibido ataques del tipo ransomware donde el malware bloquea la pantalla o **cifra la información almacenada en el disco y discos de red** y se solicita un rescate a la víctima con los detalles para efectuar el pago.

Estas son las medidas básicas que nos pueden ayudar a protegernos:

- Copias de respaldo.
- Sistemas operativos actualizado y con antivirus.
- Contraseña y autenticación.
- Correo electrónico

> **Ponte en contacto con nosotros**
>
> Si a pesar de estas recomendaciones tu equipo ha sido infectado o sospechas que pueda estarlo, desconéctalo de la red para evitar que se propague y ponte en contacto con nosotros lo antes posible.
>
> atencionsi@usal.es o llamando al 923 294500 ext 1111



Copias de respaldo.

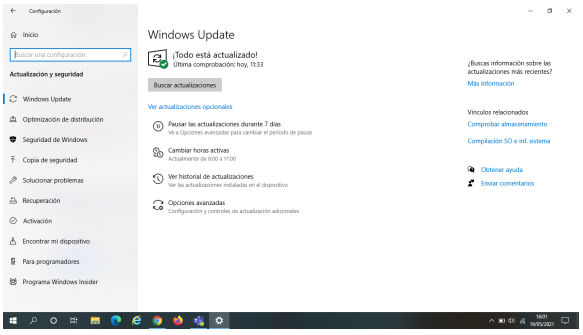
Haz copia de seguridad de tus datos importantes.
Para ello puedes copiar estos datos en un disco externo que no esté conectado al ordenador de manera habitual (tenlo sólo conectado cuando vayas a hacer la copia).
Si tu ordenador se conecta a un servidor de ficheros a través de carpetas compartidas o una unidad de red, ten en cuenta que el ramsonware lo cifrará como otra carpeta más.

En caso de tener almacenados los datos en google drive y nuestro ordenador esté conectado a la unidad G:/ u otra unidad de red, el ransomware podrá empezar a cifrar o borrar archivos, pero se podrán recuperar ya que:

- Todos los archivos almacenados en Google Drive se versionan automáticamente y se pueden restaurar a la versión anterior.
- Los archivos originales eliminados existen hasta que se vacían de la Papelera de reciclaje de Google Drive y se pueden restaurar en cualquier momento (antes de 30 días)

Sistemas operativos actualizado y con antivirus.

1. Tener el sistema operativo actualizado**.**
    a. En **windows 10** puedes comprobarlo en: **Configuración > Actualización y Seguridad > Windows UPDATE.**



2. Tener el antivirus instalado y configurado.
    a. **Antivirus ESET**
3. No instalar software no corporativo.

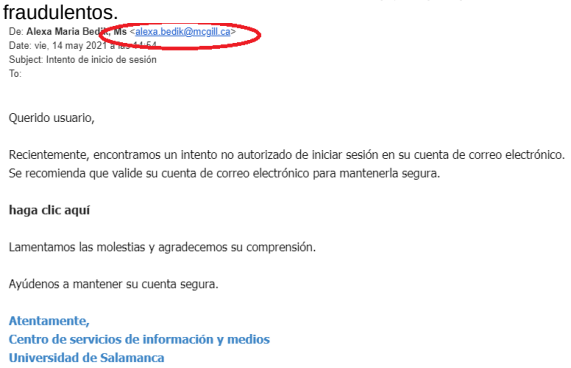
Contraseña y autenticación.

1. Ante cualquier sospecha procede a cambiar la contraseña Cambiar la contraseña y recuerda usar contraseñas seguras (mayúsculas y minúsculas, letras y números ...)
2. No registrarse en los sitios fuera de la USAL (Amazon, Netflix ...) con la cuenta xxxxx@usal.es y JAMÁS usar la contraseña de nuestras credenciales de la USAL fuera de idUSAL.

> Pero lo más seguro de todo es usar el Segundo factor de autenticación de la USAL con latch

Correo electrónico

1. En el correo electrónico ten cuidado con los adjuntos y enlaces (sobre todo si te parece extraño o es de un remitente desconocido) ya que pueden contener malware o redirigir a sitios fraudulentos.


De: **Alexa Maria Bedik, Ms** <alexa.bedik@mcgill.ca>
Date: vie, 14 may 2021 a las 14:54
Subject: Intento de inicio de sesión
To:

Querido usuario,

Recientemente, encontramos un intento no autorizado de iniciar sesión en su cuenta de correo electrónico.
Se recomienda que valide su cuenta de correo electrónico para mantenerla segura.

haga clic aquí

Lamentamos las molestias y agradecemos su comprensión.

Ayúdenos a mantener su cuenta segura.

Atentamente,
Centro de servicios de información y medios
Universidad de Salamanca

Si quieres saber más sobre el tema:

https://www.incibe.es/

https://www.eset.com/es/caracteristicas/ransomware/

https://support.google.com/drive/answer/7397771?hl=es