Seguridad en la Red

Programa «Conecta en Rural. Mujeres, digitalización y formación en la España rural. Rompiendo la brecha»

Organiza

AFAMMER

Subvenciona

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES Y AGENDA 2030

POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

INTRODUCCIÓN

- El hecho de conectarnos a Internet conlleva una serie de riesgos, lo cual es inevitable.
- Los riesgos son desde virus o malware, a la suplantación de identidad, el robo de contraseñas y datos personales, la invasión de la privacidad, etc.
- Lamentablemente, conseguir el 100% de seguridad y privacidad en la Red es imposible.
- Pero podemos tratar de mitigar los riesgos a través de ciertas medidas y con mucho sentido común. Hay que estar alerta.

INTRODUCCIÓN

Algunas cosas a tener en cuenta:

- Los estafadores pueden crear sitios web que se parezcan a uno genuino y pedirte que inicies sesión con tu dirección de correo y contraseña.
- Comprueba siempre que la URL del sitio web sea correcta antes de introducir tu información de inicio de sesión. Si tienes dudas, entra de forma directa a la página web desde el navegador y así podrás estar seguro de estar en la página correcta.
- Seguridad relacionada: si te vas de viaje, no lo publiques al momento, les estarás avisando a los ladrones que no estás en casa.

PHISHING: problema muy frecuente

Es uno de los problemas más habituales porque es muy difícil caer en la trampa.

- ¿Qué es el phishing? Phishing significa pescar en inglés. Se le ha puesto este nombre porque esta amenaza es muy parecida a eso: los atacantes utilizan un cebo virtual en forma de mensaje un enlace para atraer al usuario a hacer clic en ese enlace.
- Estos mensajes llegan en la forma de correo electrónico (el más habitual), o de mensajes de texto en un teléfono, a través de las redes sociales, etc.
- Desgraciadamente, si picas, lo más probable es que te encuentres con problemas, que pueden llegar a ser muy molestos, e incluso costarte mucho dinero.

PHISHING: problema muy frecuente

- Es muy habitual que la gente caiga en estas trampas: los atacantes hacen lo posible por engañarte.
- El mensaje parecerá provenir de una entidad fiable. Y si además el atacante está bien armado con algún conocimiento sobre ti (como los servicios a los que estás suscrito) puede parecer aún más creíble porque parece provenir de una empresa que utilizas. Esto no hace más que aumentar la posibilidad de que piensas que es un mensaje genuino.
- Además, los mensajes de phishing suelen tratar de darte la sensación de que es un mensaje urgente, que necesita tu intervención, lo que hace que la gente pinche más rápidamente y caiga en la trampa.

PHISHING: ejemplo 1

PHISHING: ejemplo 1

- Este ejemplo es un ataque de phishing cuyo objetivo es infectar tu dispositivo con un virus. Un virus puede desde ralentizar tu equipo, a encriptar todos tus datos para que los pierdas y pedir un “rescate” económico para recuperarlos, y hasta tomar el control absoluto de tu dispositivo y hacer con él lo que quieran.
- Este es el ejemplo: puedes recibir un mensaje que supuestamente es de tu compañía de la luz, en la que pone que no has pagado algo y que si no reaccionas te cortarán la luz.
- Este mensaje suele ir acompañado de la supuesta factura impagada, a través de un adjunto o un email, que en realidad lo único que hace es infectar tu equipo en el momento que le pinches.
- Si pinchas, aunque sea por curiosidad, tendrás un problema.

PHISHING: ejemplo 1

- La supuesta factura será en realidad un archivo .exe, que es un ejecutable que se usa para instalar programas, en vez de un pdf, que es lo habitual para una factura.
- ¿Qué puedes hacer para evitar esto?
  - Comprueba el email desde el que procede el correo.
  - Pregunta directamente a tu compañía eléctrica por email o por teléfono.
  - Fíjate en el formato del adjunto: si es .exe ni se te ocurra pinchar.

PHISHING: ejemplo 2

PHISHING: ejemplo 2

- Este ejemplo es un ataque de phishing cuyo objetivo es robar tus datos de inicio de sesión.
  - Ejemplo: recibes un email que dice algo así como "Siga este enlace para iniciar sesión y restablecer su contraseña AHORA porque su cuenta ha sido comprometida y sus datos de pago están en peligro".
  - La ironía es que si haces clic en ese enlace y caes en la trampa, lo que estarás haciendo será precisamente darles tus datos de acceso.
  - En este caso, el método es que se te presentará un portal de acceso falso (probablemente bastante convincente ya que se parecerá al real). Cuando introduzcas tu contraseña y otros datos personales, te los robarán y tu cuenta estará en grave peligro.

PHISHING: ejemplo 2

- El delincuente tendrá tu nombre de usuario y contraseña y podrá entrar en tu cuenta, suplantar tu identidad y cambiar tu contraseña para bloquearte y que no puedas volver a entrar.
- Según los datos de qué plataforma te hayan robado, las consecuencias de esto podrían ser catastróficas.
- Si entran en tu mail podrían cambiar todas las contraseñas de casi todos tus sitios ya que podrán darle a “cambiar la contraseña” y recibir el código de confirmación en tu email.
- Lo peor de todo es que consigan tus datos de acceso a tu banca online. Ahí ya os podéis imaginar… lo más probable es que vacíen tu cuenta en cuestión de segundos.

PHISHING: conclusion para evitarlo

- En general, para evitar ser víctima de un ataque de phishing hay que **estar atentos a los signos sospechosos**. Por ejemplo:
  - Faltas de ortografía
  - Frases extrañas (como que parezcan escritas por una persona si no una máquina.
  - Mensajes que están insuflando urgencia con palabras como “ahora mismo”, o “tienes x días para reaccionar”.
  - Mensajes que tengan adjuntos.

PHISHING: conclusion para evitarlo

Por otro lado, las **precauciones** que debes tomar son:

- Si no estás seguro de un mensaje ponte en contacto directamente con el remitente para preguntarle si realmente te ha escrito eso, antes de pinchar en ningún sitio.
- Incluso si un mensaje parece provenir de tu jefe o de un amigo cercano, y te piden datos o que inicies sesión, no te fíes: su dirección de correo electrónico o sus datos podrían haber sido suplantados.
- Del mismo modo, si recibes un mensaje que dice ser de, por ejemplo, Amazon o Facebook, puedes acceder a tu cuenta de tu forma habitual para ponerte en contacto directamente con la compañía para revisar la validez de cualquier comunicación.
- Activa la autenticación en dos pasos.

AUTENTICACIÓN EN DOS PASOS

- La **autenticación en dos pasos** te obliga a verificar tu identidad dos veces.
- Es verdad que puede ser molesto tanto rollo para iniciar sesión, pero sin dudas es una buena medida de seguridad.
- Con este método no bastará con tener solo una contraseña para iniciar sesión, sino que además necesitarás una segunda forma de verificación, normalmente un código que te envían al móvil o a tu email.
- Esto te ayudará a saber que alguien está tratando de entrar en tu cuenta, ya que te llegará el código, mientras que el atacante no podrá entrar sin ese código.
- También es interesante activar las **alertas por inicio de sesión** que tienen muchas páginas y redes sociales, ya que te mandarán un aviso cada vez que alguien trate de iniciar sesión, incluyendo además la ubicación y el tipo del dispositivo que está tratando de entrar en tu cuenta.

OTROS EJEMPLOS

- Llamadas por teléfono supuestamente de Microsoft y te vacían la cuenta.
- Robo y pérdida de cuenta de Instagram o Facebook a través de un menaje con un enlace.
- Meter tu número de teléfono en una página web y que te suscribas a algo pagando. El cargo aparece en la factura del móvil. Esto en realidad no termina de ser un virus, pero te costará dinero.

CONSEJOS DE SEGURIDAD VARIOS

- **Instala un antivirus y mantenlo actualizado.**
- **Mantened también actualizadas tus aplicaciones, tu sistema operativo, los navegadores…**
- **Cierra sesión** cuando utilices un ordenador que compartas con otras personas
- **NO le des a guardar contraseña en ordenadores ajenos.**
- **No aceptes solicitudes de amistad** de personas **sospechosas**.
- **No hagas nunca clic en enlaces sospechosos** aunque procedan de un amigo o de una empresa que conozcas. Nadie con buenas intenciones te va a pedir por correo electrónico tu contraseña.

CONSEJOS PARA CONTRASEÑAS

- **No uses la misma contraseña para todo (**si te la roban para uno de los sitios, podrían acceder a todos).
- **Contraseña segura**:
  - Es aconsejable usar alguna letra en mayúscula, así como un signo de puntuación (como @, *, #, etc).
  - Longitud mínima de 8 caracteres.
  - Tu contraseña debe ser difícil de adivinar, así que no incluyas tu nombre ni palabras normales.
- **Cambia la contraseña de vez en cuando.**
- **No compartas nunca tu contraseña** e información de inicio de sesión.
- **Cierra sesión** cuando utilices un ordenador que compartas con otras personas (lo repito porque es importante).
- **NO le des a guardar contraseña en ordenadores ajenos.**

OTRAS COSAS A TENER EN CUENTA

HTTPS

- Que ponga **https** en la URL (dirección de la página web) es lo más seguro.
- ¿Por qué? Pues porque existen muchos “hackers”, o ladrones virtuales, que están siempre atentos a ver qué pueden pescar por la red. Son expertos en informática capaces de hackear distintas páginas web.
- El HTTPS trata de frenarlos un poco, ya que es más seguro que el HTTP (sin “s”). Esto es debido a que el protocolo HTTPS hace que los datos de la página web viajen encriptados.

OTRAS COSAS A TENER EN CUENTA

Cuidado con las redes inalámbricas gratuitas y públicas

- Los puntos de acceso gratuitos son algo que agradecemos mucho ya que nos dan Internet en lugares donde no tenemos nuestra propia WiFi, o no tenemos cobertura de los datos móviles, o simplemente no queremos gastar datos.
- Encontramos a día de hoy redes WiFi gratuitas y públicas en lugares como restaurantes, hoteles, aeropuertos, estaciones de tren, etc.
- Ahora bien, no hay que olvidar que está más que comprobado que los ciberdelincuentes lo tienen más fácil a la hora de atacarnos si estamos usando una de estas redes.
- Por lo tanto, pudiendo conectar los datos del móvil, siempre que sea posible, esto es preferible.
- En caso de usar redes WiFi públicas, haced solo para cosas que no supongan un gran riesgo. Usar redes sociales desde la app, donde ya habéis iniciado sesión, pues bueno.. Vale. Pero que no se os ocurra hacer banca online desde una red inalámbrica pública.

PRIVACIDAD

- Como habéis visto, la privacidad es algo muy importante.
- Aquí entran dos factores importantes.
- Por un lado, está el tema tradicional: no queremos que los desconocidos tengan acceso a nuestros datos privados, conozcan a nuestros seres queridos, o incluso nuestra fecha de nacimiento, por dar algunos ejemplos.
- Por otro lado, los problemas de privacidad, se traducen en que los atacantes van a tener más datos para tratar de engañarnos, como por ejemplo en ataques de phishing, ya que el hecho de saber ciertas cosas nos puede hacer pensar que se trata de empresas reales, o de un amigo real.
- Igualmente, no queremos que otra persona, por mucho que sus intenciones no sean las de enviarnos un virus o robarnos nuestra cuenta, puedan entrar en nuestra cuenta: de ahí la importancia de cerrar sesión.
- Veamos un par de cosas relacionadas con la privacidad.

PRIVACIDAD – MODO INCÓGNITO

Modo incógnito de los navegadores

- Cuando se usa un navegador de Internet (Google Chrome, Mozilla Firefox, Microsoft Edge, etc.), podemos aprovechar en ciertos casos el Modo Incógnito.
- El modo incógnito es una función que es como una sesión temporal de navegación privada a la hora de usar el navegador.
- De esta manera, no se comparten datos con el navegador, no se guarda información sobre páginas web, ni el historial de navegación, contraseñas, información de formularios, cookies, etc., ya que cuando finalizas dicha sesión todos datos quedan borrados.
- Si no quieres que nadie sepa qué has estado haciendo con en Internet, usa el Modo Incógnito.
- Ojo que esto también significa que tú luego tampoco vas a poder comprobar nada de lo que estabas haciendo.
- *Ejemplo práctico de cómo activar el modo incógnito o privado.*

PRIVACIDAD - VPN

Otro gran jugador aquí son las **VPN**, tal vez lo hayáis escuchado alguna vez.

- Tratando de explicar de forma sencilla qué es una VPN: Cuando haces uso de internet, tus datos transitan por la red. Una VPN lo que hace es **redirigir tu tráfico a través de un túnel seguro**, enmascarando tu IP (que es un identificador que apunta directamente a tu dispositivo) y encripta tus datos.
- Como resultado, estos datos se protegen, tu privacidad se asegura y estarás más a salvo de ataques de cibercriminales o hackers.

VPN

- Por lo tanto, una VPN te ayuda a proteger tu seguridad y privacidad.
- Es algo adicional al antivirus. Para instalar una VPN, que hay gratuitas y de pago, debes instalar un programa que descargarás desde la página oficial de la VPN que escojas.
- Por cierto, la VPN también te ayudará si vas a usar redes inalámbricas públicas, ya que al “esconder” tus datos en la red en ese túnel seguro, hace más difícil que alguien ajeno pueda acceder.
- Podéis encontrar más información sobre las VPN pinchando en este enlace.

AFAMMER

GOBIERNO DE ESPAÑA
MINISTERIO DE DERECHOS SOCIALES Y AGENDA 2030
POR SOLIDARIDAD
OTROS FINES DE INTERÉS SOCIAL

ESPERAMOS QUE LOS CONTENIDOS TE SEAN DE UTILIDAD
¡¡HASTA PRONTO!!