Contenido Unidad

[Flujo de informacion y Comunicación online]

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: bit schulungscenter
Last processing date: 14.08.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Flujo de informacion y Comunicación online

Introducción

Internet ha tenido un gran impacto en la manera que tenemos de comunicarnos con los demás. Para muchos de nosotros, la comunicación online es simplemente parte de nuestro día a día. Incontables emails se abren, reenvían y responden cada día. De esta manera, la informacion puede enviarse de manera rápida, sencilla y efectiva. ¿Tu servidor de correo no funciona correctamente? ¡Naveguemos por internet! Es sencillo encontrar un foro donde alguien describe problemas similares y otros usuarios comparten consejos útiles con el resto de la comunidad. Como puedes ver, no hay duda de que la comunicación online ofrece muchas ventajas. Sin embargo, el uso diario de correos y otros medios de comunicación electrónicos, que damos por garantizados, nos lleva a despreocuparnos y esto a reconocer los riesgos potenciales o a no reconocerlos en absoluto. Esto hace que sea muy importante conocer a qué deberíamos poner atención cuando estamos utilizando la comunicación online para reducir riesgos de consecuencias negativas.

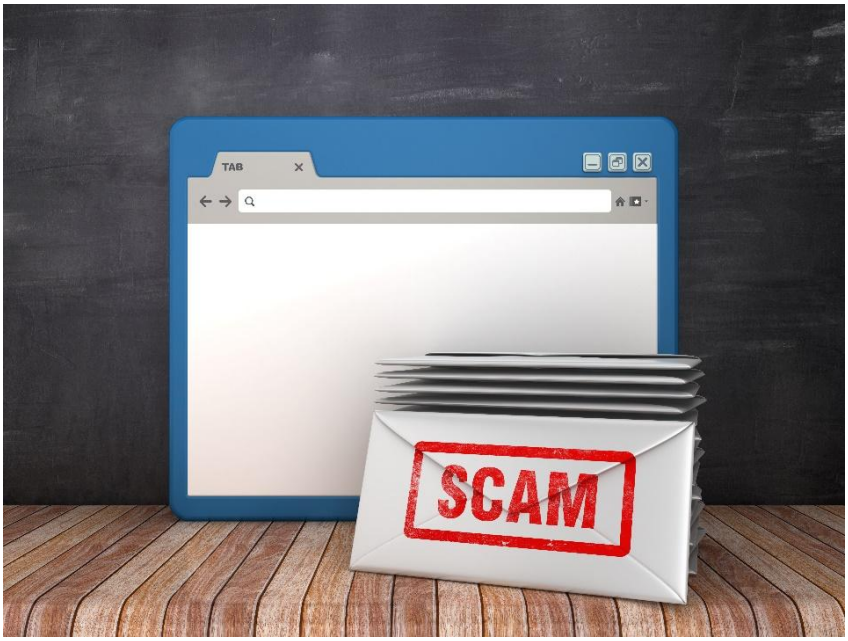
Importancia práctica– ¿Para qué necesitas estos conocimiento y habilidades?

La incipiente utilización de Internet y de numerosas herramientas de comunicación electronica, tanto en nuestras vidas personales como en el entorno professional, está creando amenazas adicionales a la seguridad de nuestros datos y a nuestra privacidad. Por tanto, es importante conocer los riesgos actuales en la protección de datos para ser capaces de reconocerlos rápido y responder correctamente si fuera necesario. En tiempos como los actuales, en los que el cibercrimen está creciendo, contar con el conocimiento sobre los posibles problemas de seguridad en el curso de la comunicación online, así como sobre la correcta utilización del correo electrónico, deben ser obligatorios para cualquier usuario.

1. Construye conocimiento- Emails y contenidos adjuntos falsos

El medio más popular para la comunicación online es el email. Abrir y enviar emails es parte de tu rutina diaria, ¿verdad? Pero precisamente por su elevada popularidad, los emails falsos son una amenaza muy común también.

Co-funded by the
Erasmus+ Programme
of the European Union



Definición

Los emails falsos son emails indeseados que te inducen a error a mala fe con informacion engañosa o que te llevan a realizar acciones perjudiciales. Por ejemplo, software malicioso se transfiere a menudo a través de emails falsos en su contenido adjunto.

Por tanto, es importante estar al tanto de las características típicas de los emails maliciosos. Antes de abrir los adjuntos, clicar en los enlaces o responder correos electrónicos, puede ser de ayuda realizarte las siguientes preguntas:

1. ¿Te promete algo demasiado bueno para ser real? Ten cuidado: si es **demasiado bueno para ser verdad**, casi seguro que no será real.

Ejemplo

Ejemplos de ello son emails con chicas atractivas que quieren conocerte, regalos gratuitos o la notificación de que has Ganado un premio (aunque no hayas participado en ningún sorteo).

2. ¿El contenido del correo de alguna manera **no encaja con el supuesto emisor**?

Ejemplo

Recibes un email de tu amiga Anna. Ella escribe que está de vacaciones en el extranjero y que ha sido víctima de un robo. Por ello, te pide que le transfieras dinero inmediatamente a una cuenta para que pueda coger el ultimo avión a casa esta semana.
Un contenido como este indica claramente que la cuenta de email de Anna ha sido hackeada.

3. ¿El email contiene **palabras dentro del asunto** como “ultimo recordatorio”, “cuenta bloqueada” o similares? ¿Te piden que divulgues tus datos de acceso, contraseñas u otra **informacion confidencial**?

Importante

¡Cuando alguien te mete prisa para que divulgues informacion confidencial, debería encender las alarmas!

4. ¿El **emisor parece extraño** (por ejemplo, un email en inglés procedente de una empresa alemana)? ¿Contiene muchos **errores tipográficos o gramaticales** (probablemente debidos a programas de traducción automática)?

5. ¿El email se ha enviado automáticamente a la **carpeta de spam**?

Puedes estar preguntándote ahora, para qué pensar en los emails de la carpeta de spam. Muchos proveedores de correo electrónico están constantemente mejorando su monitorización automática y por tanto los emails indeseados acaban en dicha carpeta. Sin embargo, el problema es que también puede haber emails que, por error, sean considerados como no deseados y acaben en la carpeta de spam.

Ejemplo
Tu amigo va a tener una gran fiesta por su cumpleaños. Envía las invitaciones por email a muchos invitados simultáneamente metiendo todas las direcciones de email en copia. Desafortunadamente, es posible de que tu invitación acabe en la carpeta de correo no deseado, ya que contra con muchas direcciones en copia es una señal típica de spam.

6. ¿Te piden ejecutar programas con nombres de archivo extraños (por ejemplo, sumas de varios nombres de archive como jpg.vbs o gif.exe)?

Si has contestado “sí” a una o más de estas preguntas, o si un email te resulta sospechocho por otras razones, **no debes abrir el email** o los archivos y enlaces que contiene.

El famoso **pishing** requiere de especial cuidado.

Definición
El término **phishing** consiste en la suma de las palabras "password" (contraseña) y "fishing" (pescar). El phishing es el intento de **obtener contraseñas** mediante la ayuda de emails falsos.

Puede que hayas recibido alguna vez un **email extraño** de tu banco o de alguna tienda online que conozcas. En muchos casos te informarán de que, desafortunadamente, tus datos de usuario se han perdido o de que tu contraseña ha expirado o de que se requiere una nueva identificación urgentemente debido a una actualización. Convenientemente, con frecuencia se envía un **enlace directo a la página web** de la compañía. Estas páginas parecen **muy similares** a las originales, pero son **falsas**. Si introduces tus datos bancarios en buena fe, los estafadores tendrán acceso a ello y pueden perjudicarte.

Consejo
Los correos en los que se requiere que envíes tus datos de usuario nunca deben ser contestados. Las compañías serias no te pedirían eso. Si todavía no estás seguro, tiene sentido preguntar al presunto emisor por teléfono.

Además, las siguientes medidas pueden ayudar a **reducir el riesgo** en la comunicación online a través del correo electrónico:

- Activa la **pantalla de extensión de archivos**. Esto te permite identificar mejor programas maliciosos enviados como contenido adjunto (por ejemplo .docx, .exe).
- Utiliza los ajustes de seguridad apropiados para prevenir la ejecución de contenido activo en los programas de correo electrónico. Por ejemplo, puedes prevenir que el **malware no deseado** se ejecute cuando se abra un email.
- **Guarda los contenidos adjuntos sospechosos antes** de abrirlos para poder pasarle un programa antivirus.

1. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Asociado al objetivo específico: OE_01_01

Situación: ¿A qué nos referimos mediante el término “email falso”?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Los emails falsos son emails no deseados que a menudo contienen malware enviado en el contenido adjunto.
- Los emails falsos proveen información falsa o no verdadera.
- Los emails falsos pueden incluso no haber sido enviados por el supuesto remitente.
- Los emails falsos son correos sin ningún contenido. Estos emails vacíos se envían intencionadamente o de manera accidental.

Ejercicio OPCIÓN MÚLTIPLE

Asociado al objetivo específico: OE _01_02

Situación: Compruebas tu bandeja de correo electrónico y tienes muchos emails nuevos. ¿Cuál de los siguientes casos tiene una alta probabilidad de ser un email falso?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Te prometen una gran recompensa.
- Te piden que cambies urgentemente tus datos de acceso.
- El email no tiene asunto.
- El asunto es un último aviso.
- El email contiene un buen número de errores gramaticales.
- El email acabó directamente en la bandeja de correo no deseado.
- El email fue enviado de madrugada.

Ejercicio OPCIÓN MÚLTIPLE

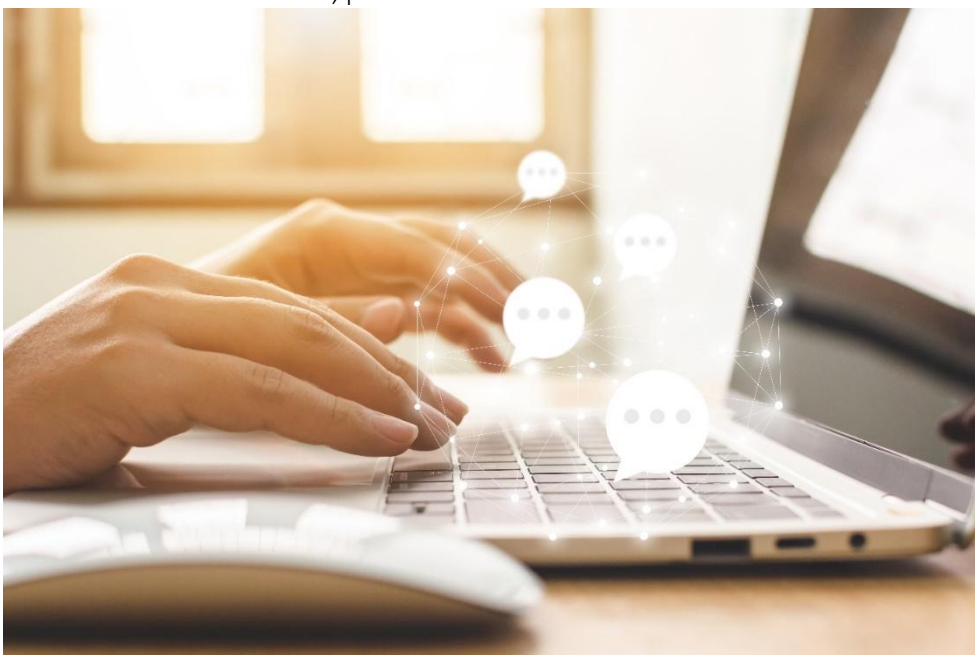
Asociado al objetivo específico: OE

Situación: ¿Qué medidas pueden ayudarte a reducir los riesgos de la comunicación online vía correo electrónico?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Activar la pantalla de extensiones de archivo (p.e. .docx, .exe).
- Desactivar la pantalla de extensiones de archivo.
- Usar los ajustes de seguridad apropiados para prevenir la ejecución de contenido activo en los programas de correo electrónico.
- Escanear el contenido adjunto sospechoso por un programa antivirus.
- **Difundir solamente tus datos de usuario en el caso de que conozcas muy bien a las empresas que te los están requiriendo.**

2. Construye conocimiento – Foros y salas de chat

Tanto los **foros** como las **salas de chat** son medios muy populares para la comunicación online y el intercambio de información, pero difieren en la manera de utilizarse.



Definición
Las salas de chat suelen estar enfocadas en la comunicación en **tiempo real**, mientras que, en los foros, frecuentemente, las discusiones se producen entre **participantes que no se encuentran necesariamente online al mismo tiempo**. Los foros se encuentran normalmente mejor organizados, con discusiones divididas por hilos que son moderados.

Los chats y foros permiten el intercambio de mensajes de texto, pero normalmente también se puede intercambiar imágenes, vídeos, enlaces o archivos. Además, algunas salas de chat permiten también la utilización de micrófonos o webcams para chatear con otros usuarios.

Para participar activamente en foros y chats se requiere normalmente **registrarse con una dirección de correo electrónico** válida. Esto es para prevenir el spam en los posts. Por otro lado, los moderadores tienen también la posibilidad de suspender o bloquear a usuarios en foros y chats si se comportan de manera inapropiada. No obstante, el uso de estos medios de comunicación puede implicar varios riesgos y amenazas, entre los que se incluyen, por ejemplo:

- **Malware o enlaces a sites de phising:** Todos los archivos y enlaces que se postean en foros deberían por ello ser tratados con cautela
- Debes tener en mente que cuentas falsas o hackers pueden inducirte a confiar en **identidades falsas**.
- La comunicación en foros y chats normalmente es **completamente desencriptada**, por lo que tus declaraciones y comentarios pueden ser leídos por cualquier usuario. Cualquier profesional puede leer también sin problemas cualquier mensaje privado

¿No quieres dejar de participar en foros y chats y te estás preguntando qué puedes hacer para evitar riesgos de seguridad? La consideración de los siguientes aspectos es, desde luego, un paso importante.

- No abras sin criterio los archivos que te envíen.
- Nunca envíes datos personales sensibles a gente que no conozcas personalmente.
- **Nunca permitas a nadie que accede a tu ordenador,** incluso durante una sesión de chat.

Ejemplo
Tienes un problema en el ordenador y estás buscando consejo en un chat de expertos. Un supuesto experto quiere ayudarte y, para ello, te pide acceso remoto al control de tu ordenador.

- Debes leer los **términos y condiciones generales** y el **reglamento de protección de datos** correspondiente al servicio, particularmente en lo que se refiere a lo que ocurre con tus datos e información. ¿Se venden? ¿Se almacenan? ¿Se encriptan?
- **Bloquea contactos** si no estás seguro de quiénes son o si alguien te está acosando. Denuncia a la policía los insultos, el acoso sexual, el chantaje o las amenazas.
- No te olvides del **copyright**: no deberías enviar fotos u otros archivos que no hayas creado tú mismo sin el permiso del autor.
- Sé siempre **cauteloso cuando quedes con un extraño** a quien solo conozcas de foros o chats. Incluso si tienes la impresión de que ya le conoces personalmente, la informacion que te haya dado puede ser falsa o inventada.

2. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Asociado al objetivo específico: OE_02_01

Situación: ¿Qué son salas de chat y qué entendemos por foros? ¿En qué se diferencian ambas herramientas de comunicación?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Las salas de chat son muy proclives a las conversaciones en las que ninguno de los participantes tiene por qué encontrarse online al mismo tiempo.
- Los foros se encuentran mejor preparados que los chats para conversaciones en tiempo real.
- Los mensajes de texto pueden intercambiarse tanto en salas de chat como en foros. A menudo, puedes intercambiar también fotos, vídeos, enlaces o archivos.
- Las salas de chat se encuentran mejor preparadas que los foros para las conversaciones en tiempo real.
- En las salas de chat puedes hablar anónimamente bajo un seudónimo, mientras que en los foros tienes que divulgar tu nombre real.

Ejercicio OPCIÓN MÚLTIPLE

Asociado al objetivo específico: OE _02_02

Situación: Foros y salas de chat son herramientas muy populares para la comunicación online. Sin embargo, ¿a cuáles de los siguientes riesgos te enfrentas utilizándolos?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Ser infectado por software malicioso cuando abres archivos compartidos en salas de chat o foros.
- La redirección a sitios de phishing cuando clicas en enlaces compartidos.
- Que de repente incurras en costes muy elevados al intercambiar mensajes en foros.
- Que alguien esté intentando engañarte para que confíes en una identidad falsa.
- Que los mensajes que envíes en un chat sean leídos también secretamente por terceros.

Ejercicio OPCIÓN MÚLTIPLE

Asociado al objetivo específico: OE _02_0

Situación: ¿Cuáles de las siguientes medidas puedes tomar para reducir el riesgo dentro de la comunicación online a través de chats y foros?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Leer los términos y condiciones generales del servicio de comunicación.
- Bloquear contactos si no estás seguro de quiénes son.
- Compartir solamente fotos o archivos que no hayas creado tú mismo.
- Permitir solamente acceder a tu ordenador a aquellos que tengan nombres de usuario y fotos de perfil que inspiren confianza.
- No abrir sin criterio archivos que te hayan enviado.

3. Construye conocimiento – Comunicación a través de las redes sociales

En las redes sociales, la presunción de anonimato puede llevarnos a comportarnos sin pensar en lo que se refiere a los datos e información. Como resultado, se ha producido un crecimiento de las actividades fraudulentas en las redes sociales.

Debes considerar siempre los siguientes aspectos cuando trates con los medios sociales:

- Nunca publiques ni compartas información personal o confidencial en un espacio público virtual. Puede traer consecuencias legales si publicas afirmaciones desconsideradas o no probadas.
- Toda red social tiene la opción de hacer la información personal solamente pública a algunas categorías de grupos de persona mediante filtros. Comprueba dichas opciones para que nunca debas correr el riesgo de tener que dar la bienvenida a miles de extraños a tu fiesta de cumpleaños.
- ¿Te gusta tener tantos amigos como sea posible en tus redes sociales? Ten cuidado de no olvidar el dicho: “Dime con quién andas y te diré cómo eres”. **Aceptar amigos sin pensar puede tener consecuencias negativas sobre ti**. Por ejemplo, cuando estás buscando trabajo. Muchos empleadores se informan sobre las actividades en redes sociales de los que han

solicitado el puesto y utilizan dicha información para tomar decisiones en el proceso de selección.

- Comprueba siempre las opciones de privacidad de las redes sociales sobre la política de privacidad.
- Ten en cuenta que en las redes sociales hay un especial riesgo de engaño. Los defraudadores engañan deliberadamente y manipulan a sus víctimas proveyéndoles de información potencialmente peligrosa.

Importante
Si detectas una utilización incorrecta o inapropiada de las redes sociales, debes denunciarlo al proveedor del servicio y a las organizaciones y autoridades apropiadas

3. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Asociado al objetivo específico: OE _03_01

Situación: ¿Qué deberías considerar cuando estés utilizando las redes sociales para evitar las posibles consecuencias negativas?

Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Aceptar tantas peticiones de amigos como sea posible para hacerte parecer muy popular para los demás.
- Comprueba siempre los ajustes sobre protección de privacidad de los medios sociales.
- No te creas toda la información que recibes en las redes sociales.
- Si no te gusta alguien y quieres postear comentarios muy negativos sobre dicha persona, ten cuidado de no utilizar tu nombre real, especialmente si utilizas lenguaje duro. De esta manera puedes permanecer en el anonimato y no tienes que temer las consecuencias.

Ejercicio OPCIÓN MÚLTIPLE

Asociado al objetivo específico: OE _03_02

Situación: Estás echándole un vistazo a tu cuenta en una red social. En shock, descubres que alguien ha posteado un video en la red en el que se muestra a un grupo de adolescentes abusando salvajemente de una chica, tanto física como mentalmente. ¿Cómo deberías reaccionar?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- **Debes denunciar al proveedor del servicio (p.e. Facebook)**
- Desafortunadamente, no hay nada que puedas hacer. A lo mejor el video ni siquiera es real. Para evitar que te amenacen a ti, lo ignoras.
- **Debes denunciarlo a la policía.**
- No conoces ni a la víctima ni al que perpetra el ataque, por lo que no puedes darle a nadie un nombre concreto. Por tanto, no hay necesidad de que interfieras.

Co-funded by the
Erasmus+ Programme
of the European Union

Fuentes

wko.at: https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/chat/

onlinesicherheit.gv.at: https://www.onlinesicherheit.gv.at/gefahren_im_netz/soziale_medien/gefahren/250080.html

securitymetrics.com: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

ftc.gov: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

smallbusiness.com: https://smallbusiness.chron.com/differences-between-chat-rooms-forums-71296.html

socialnomics.net: https://socialnomics.net/2017/11/08/chatting-online-risks-the-tips-to-stay-safe/

getsafeonline.org: https://www.getsafeonline.org/social-networking/chatrooms/

cybersecurity.edu: https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/social-media

Afianza conocimiento

Resumen

La forma más popular de comunicación online es el correo electrónico, que es lo que lleva a que los emails falsos sean también muy populares. Los **emails falsos** son correos no deseados con informacion maliciosamente falsa o engañosa. Por ejemplo, el **malware** se esconde a menudo en los **adjuntos** de estos correos falsos.

Para no caer en estos emails falsos, es importante **estar alerta**. Por ejemplo, los correos que te ofrecen una gran ganancia o que te piden revelar informacion confidencial han de ser siempre tratados con cautela. Esto mismo aplica a correos con asuntos como “Tu cuenta bancaria ha sido bloqueada” o con una cantidad inusual de errores gramaticales o de faltas de ortografía. I

Hemos de tener especial cuidado con los famosos **correos phising**, donde los emails falsos se utilizan para obtener contraseñas. Para reducir el riesgo en nuestra comunicación online, tiene sentido guardar los adjuntos sospechosos de los correos y **escanearlos a través de un programa antivirus.**

Existe también el riesgo de infectar tu ordenador con malware o ser reenviado a sitios de phising clicando sin cuidado en enlaces o abriendo archivos cuando nos **comunicamos a través de foros o chats**. Otros peligros relacionados a tener en cuenta son las falsas identidades o la lectura involuntaria de nuestros mensajes.

Por tanto, resulta de particular importancia leer cuidadosamente **el reglamento de protección de datos** de los proveedores de comunicación y no desvelar jamás **informacion personal o sensible en chats o foros**.

Esto aplica también cuando estamos utilizando las redes sociales. Ten en cuenta que en las redes sociales existe un riesgo especial de ser engañado por **identidades falsas** o por la **divulgación consciente o inconsciente de información falsa**. Si detectas una conducta inapropiada o incorrecta en las redes sociales, **puedes y debes** denunciarlo al proveedor de servicios y a las organizaciones y autoridades pertinentes.

Las respuestas correctas están marcadas en negrita

Situación: ¿A qué nos referimos mediante el término "email falso"?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- **Los emails falsos son emails no deseados que a menudo contienen malware enviado en el contenido adjunto.**
- **Los emails falsos proveen información falsa o no verdadera.**
- **Los emails falsos pueden incluso no haber sido enviados por el supuesto remitente.**
- Los emails falsos son correos sin ningún contenido. Estos emails vacíos se envían intencionadamente o de manera accidental.

Situación: Compruebas tu bandeja de correo electrónico y tienes muchos emails nuevos. ¿Cuál de los siguientes casos tiene una alta probabilidad de ser un email falso?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- **Te prometen una gran recompensa.**
- **Te piden que cambies urgentemente tus datos de acceso.**
- El email no tiene asunto.
- **El asunto es un último aviso.**
- **El email contiene un buen número de errores gramaticales.**
- **El email acabó directamente en la bandeja de correo no deseado.**
- El email fue enviado de madrugada.

Situación: ¿Qué medidas pueden ayudarte a reducir los riesgos de la comunicación online vía correo electrónico?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- **Activar la pantalla de extensiones de archivo (p.e. .docx, .exe).**
- Desactivar la pantalla de extensiones de archivo.
- **Usar los ajustes de seguridad apropiados para prevenir la ejecución de contenido activo en los programas de correo electrónico.**
- **Escanear el contenido adjunto sospechoso por un programa antivirus.**
- Difundir solamente tus datos de usuario en el caso de que conozcas muy bien a las empresas que te los están requiriendo.

Situación: ¿Qué son salas de chat y qué entendemos por foros? ¿En qué se diferencian ambas herramientas de comunicación?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Las salas de chat son muy proclives a las conversaciones en las que ninguno de los participantes tiene por qué encontrarse online al mismo tiempo.

- Los foros se encuentran mejor preparados que los chats para conversaciones en tiempo real.
- Los mensajes de texto pueden intercambiarse tanto en salas de chat como en foros. A menudo, puedes intercambiar también fotos, vídeos, enlaces o archivos.
- Las salas de chat se encuentran mejor preparadas que los foros para las conversaciones en tiempo real.
- En las salas de chat puedes hablar anónimamente bajo un seudónimo, mientras que en los foros tienes que divulgar tu nombre real.

Situación: Foros y salas de chat son herramientas muy populares para la comunicación online. Sin embargo, ¿a cuáles de los siguientes riesgos te enfrentas utilizándolos?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Ser infectado por software malicioso cuando abres archivos compartidos en salas de chat o foros.
- La redirección a sitios de phishing cuando clicas en enlaces compartidos.
- Que de repente incurras en costes muy elevados al intercambiar mensajes en foros.
- Que alguien esté intentando engañarte para que confíes en una identidad falsa.
- Que los mensajes que envíes en un chat sean leídos también secretamente por terceros.

Situación: ¿Cuáles de las siguientes medidas puedes tomar para reducir el riesgo dentro de la comunicación online a través de chats y foros?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Leer los términos y condiciones generales del servicio de comunicación.
- Bloquear contactos si no estás seguro de quiénes son.
- Compartir solamente fotos o archivos que no hayas creado tú mismo.
- Permitir solamente acceder a tu ordenador a aquellos que tengan nombres de usuario y fotos de perfil que inspiren confianza.
- No abrir sin criterio archivos que te hayan enviado.

Situación: ¿Qué deberías considerar cuando estés utilizando las redes sociales para evitar las posibles consecuencias negativas?

Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Aceptar tantas peticiones de amigos como sea posible para hacerte parecer muy popular para los demás.
- Comprueba siempre los ajustes sobre protección de privacidad de los medios sociales.
- No te creas toda la información que recibes en las redes sociales.
- Si no te gusta alguien y quieres postear comentarios muy negativos sobre dicha persona, ten cuidado de no utilizar tu nombre real, especialmente si utilizas lenguaje duro. De esta manera puedes permanecer en el anonimato y no tienes que temer las consecuencias.

Situación: Estás echándole un vistazo a tu cuenta en una red social. En shock, descubres que alguien ha posteado un video en la red en el que se muestra a un grupo de adolescentes abusando salvajemente de una chica, tanto física como mentalmente. ¿Cómo deberías reaccionar?
Tarea: Selecciona las opciones correctas en el siguiente test de respuesta múltiple: la opción correcta puede ser ninguna, una o más de una.

- Debes denunciar al proveedor del servicio (p.e. Facebook)

- Desafortunadamente, no hay nada que puedas hacer. A lo mejor el video ni siquiera es real. Para evitar que te amenacen a ti, lo ignoras.
- Debes denunciarlo a la policía.
- No conoces ni a la víctima ni al que perpetra el ataque, por lo que no puedes darle a nadie un nombre concreto. Por tanto, no hay necesidad de que interfieras.