04

Correo Electrónico, Chats y Mensajería Instantánea.



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



ÍNDICE

I. OBJETIVOS 3
II. CONCEPTOS 3
1. TÉRMINOS COMUNES 3
a) Dirección IP 3
b) Correo Web. 3
c) Cadena de mensajes 3
d) Correo electrónico no deseado o spam 3
e) Software malicioso 4
f) Nick 4
g) Canal de chat. 4
2. CONTENIDO. 4
a) Correo electrónico. 5
b) Mensajería instantánea y chats. 7
3. PARA SABER MÁS 8
III. ACTIVIDADES 9
1. NICK. 9
2. EL CORREO ELECTRÓNICO Y SUS RIESGOS. 9
3. CONFIDENCIALIDAD EN EL CORREO ELECTRÓNICO. 9
4. CHATS 10

CC BY SA



I. OBJETIVOS

- Aprender a hacer un buen uso de los servicios de correo electrónico, chats y mensajería instantánea.
- Conocer los riesgos para nuestros datos personales si utilizamos estos servicios sin algunas precauciones.

II. CONCEPTOS

1. TÉRMINOS COMUNES.

a) Dirección IP.

Conjunto de números que identifican un ordenador cuando se conecta a una red que utiliza el protocolo IP.

b) Correo Web.

Sistema de acceso al correo electrónico que se realiza utilizando el navegador de Internet y el *protocolo http*. Existen numerosos proveedores de servicio de Internet que ofrecen este servicio de forma gratuita o con coste reducido.

c) Cadena de mensajes.

Conocido también como cadena de correo electrónico o *hoax*, es un sistema de propagación rápida de mensajes - en muchos casos engañosos - utilizando el correo electrónico y solicitando al usuario que lo recibe que lo remita al conjunto de usuarios que conozca.

d) Correo electrónico no deseado o spam.

Mensajes de correo, habitualmente de contenido publicitario, que son remitidos a los usuarios sin que estos lo hayan solicitado previamente o hayan dado su consentimiento. En muchos casos, se difunden de forma masiva y utilizando medios ilícitos para la obtención de direcciones de correo y para el proceso de envío.



e) Software malicioso.

Virus, gusanos y otro tipo de *malware* - ***mal****icious soft****ware*** -, diseñado para insertar *troyanos* o *spyware* en sistemas de información. Son causantes de daños muchas veces irreparables y de la recogida de información confidencial en sistemas informáticos.

f) Nick.

Apodo o pseudónimo utilizado como código de usuario en chats o servicios de mensajería instantánea.

g) Canal de chat.

Salas virtuales en las que los diferentes participantes hablan de algún tema concreto.

2. CONTENIDO.

En los últimos años Internet ha evolucionado y nosotros con la Red. Hemos pasado de tener un modelo en el que el internauta ocupaba un papel pasivo, de mero lector, a un papel activo y protagonista. La Web se ha convertido en un espacio social donde los individuos interactúan y se relacionan en comunidades.

En este contexto surgen diferentes servicios que permiten que estemos en contacto con otros como son el correo electrónico, los chats y la mensajería instantánea.



a) Correo electrónico.

El correo electrónico es uno de los servicios que mayor desarrollo ha alcanzado en Internet. Nos permite enviar y recibir mensajes muy rápidamente y mantenernos conectados con otras personas. La manera de darnos de alta en servicios de correo es muy sencilla: simplemente tendremos que facilitar determinada información personal (nombre y apellidos, ciudad, etc.) y aceptar los términos de uso. Una vez tengamos nuestra dirección de correo es más que probable que la utilicemos en múltiples lugares de Internet, ya que nos lo solicitan para darnos de alta en otros servicios y sin nuestro email resultaría imposible acceder a los mismos.

Hay que tener en cuenta que la dirección de correo es la forma más común de registrar la "identidad" de una persona en Internet y que puede servir de base para la acumulación de información en torno a la misma. **Cuidar de nuestra dirección de correo es muy importante ya que dice quiénes somos en Internet**, al igual que nuestra dirección de casa nos identifica y dice quiénes somos en el mundo real.

El correo electrónico es una forma segura de comunicarse pero no hay que perder de vista algunos riesgos como:

› **La recopilación de direcciones de correo (cadenas de mensajes):**

La participación de los usuarios en cadenas de mensajes puede facilitar que las direcciones a las que reenviamos el email sean recopiladas por programas específicos o por el usuario que ha originado la cadena.

No es recomendable reenviar este tipo de correos, pero si lo hacemos es imprescindible utilizar el campo **Con Copia Oculta** (CCO) del correo electrónico (email) para evitar que las direcciones de nuestros contactos aparezcan en el cuerpo del mensaje. Así evitamos que terceros tengan acceso a esas cuentas.



› **La suplantación de identidad:**

En Internet no todo el mundo es quien dice ser. Hay que partir de la base de que este tipo de servicios no facilitan el establecimiento fiable de la identidad real del emisor o receptor del correo. Podemos recibir un email de una persona que conocemos, pero realmente no ser de esa persona, sino de un tercero que utilizando un nombre de alguien conocido contacta con nosotros.

› **La instalación de software malicioso:**

Frecuentemente recibimos en nuestra bandeja de entrada avisos relacionados con la existencia de un virus o gusano cuyo principal canal de distribución es el correo electrónico. Hay que tener cuidado al abrir estos correos, ya que normalmente su objetivo precisamente es propagar esos virus. Antes de abrir un archivo adjunto, es importante comprobar que la persona que nos envía el mensaje es conocida y realmente es esa persona, ya que los virus a veces proceden de un destinatario conocido pero al que realmente están suplantando su identidad.

Recomendaciones para el uso del correo electrónico:

› **Utilizar contraseñas seguras**. Combinar números, letras y símbolos y cambiarla de forma periódica, al menos una vez al año.

› No proporcionar la dirección de correo electrónico si no se está seguro de las intenciones de aquél que la pide. No facilitar nunca las contraseñas.

› Si se utiliza un ordenador de forma compartida, **no utilizar la opción "guardar contraseña"**.

› Cuando se envíe un correo a varios destinatarios **es mejor utilizar el campo "Con Copia Oculta",** ya que así evitaremos revelar las direcciones de otros.

› No abrir aquellos mensajes que resulten dudosos o de procedencia desconocida. Ante la duda, mejor borrarlos.



- Evita reenviar cadenas de mensajes.
- **Crea distintas cuentas de correo**. Por ejemplo, puedes utilizar una que conozcan tus amigos y familiares y otra para darte de alta en redes sociales, juegos online u otros servicios de Internet. Te resultará más fácil gestionar tus contactos y tus correos.

b) Mensajería instantánea y chats.

Los chats se engloban dentro de lo que llamamos "protocolos de mensajería instantánea". Este tipo de mensajería se diferencia del correo electrónico en que las conversaciones se mantienen en tiempo real y nos permite hablar con todos aquellos que estén conectados en una misma sala o canal de chat.

Por otra parte, para utilizar la mensajería instantánea, es necesario que instalemos en nuestro ordenador un programa.

Debemos registrarnos con usuario y contraseña y, para poder hablar con otros, es necesario haberlos aceptado previamente como amigos. Además, tendremos que crearnos un nick, que será nuestro nombre cuando estemos utilizando este servicio. En teoría, la mensajería instantánea debería ser más privada que los chat, y servir de canal de comunicación únicamente con amigos o conocidos, pero en ocasiones se acepta a personas sin tener muy claro quiénes son o directamente desconocidas.

Los chats y los servicios de mensajería nos ofrecen la posibilidad de conocer gente, contactar con amigos y compartir nuestros gustos, aficiones o conocimientos. No obstante, hay que ser conscientes de que exponer excesiva información personal en este tipo de sitios puede acarrearnos alguna consecuencia que no deseamos.

Recomendaciones para el uso de mensajería instantánea y chats:

- Cuidado al crear un *nick*. El *nick* no debe aportar información personal ni directa ni indirectamente. Ejemplo, Maria14, da a entender que tenemos 14 años y personas que pueden no tener realmente esa edad, contactar con nosotros a través de Internet con malas intenciones.



- En conversaciones abiertas en chats no facilitar nunca excesiva información personal que pueda identificarnos o incluso ubicarnos físicamente. No es nada recomendable decir dónde vivimos, a qué instituto vamos o dar datos personales como nombre completo, nuestro móvil, etc. a gente que hemos conocido a través de Internet.
- No revelar información de terceros sin su consentimiento. Igual que debemos cuidar de nuestros datos personales y privacidad, debemos cuidar de la de otros y no revelar información de amigos.
- No compartir nunca imágenes con personas que no conocemos, ni nuestras ni de amigos. Tampoco subir imágenes personales a chats abiertos donde cualquiera puede tener acceso a las mismas.
- No escribir cosas de las que nos podamos arrepentir. Pensar en cómo puede entender el otro lo que estamos escribiendo.

3. PARA SABER MÁS.

- Guía para la lucha contra el spam – AEPD:

  http://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM–ap-V.-30-mayo-cp-.pdf

- Decálogo contra el spam – AEPD:

  http://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/CONSEJOS-para-prevenir-el-Spam_guia.pdf

- Comunicación sobre las comunicaciones comerciales no solicitadas - Comisión Europea:

  http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/COMUNICACION-COM-28.pdf



III. ACTIVIDADES

1. NICK.

El educador pedirá que todos los alumnos se pongan un nick. Después podrán formar grupos e intentar adivinar a quién pertenece cada nick. Después debatirán sobre la importancia de ponerse un nick que no te pueda identificar fácilmente.

2. EL CORREO ELECTRÓNICO Y SUS RIESGOS.

El educador planteará a los alumnos el siguiente supuesto:

Eres uno de los reporteros del periódico del barrio y te has enterado de que varios conocidos han sido víctimas de un virus que se ha instalado en su ordenador. Todos sospechan que este virus se ha propagado a través de un correo electrónico. Como reportero cuenta la noticia y da algunos consejos para protegerse contra estas prácticas.

3. CONFIDENCIALIDAD EN EL CORREO ELECTRÓNICO.

Marta hace ya dos años tuvo un problema con algunas compañeras de clase. La cosa fue tan grave que estuvieron mandándole mensajes bastante feos a través de su correo electrónico. Por eso, Marta decidió no volver a utilizar esta cuenta de correo electrónico y abrirse una nueva.

Hace una semana Marta recibió un correo electrónico de una amiga que también había sido compañera de clase. Se trataba de un e-mail con algunas fotos navideñas.

El problema es que en este correo electrónico no se había tomado la "precaución" de utilizar la opción de "copia oculta" y, por tanto, se podían ver todos los correos electrónicos a los que había sido enviado. Marta se dio cuenta de que esas chicas, con las que había tenido problemas, podrían tener acceso a su nueva dirección de correo electrónico.

El educador planteará la siguiente pregunta:

1. ¿Todos conocéis la opción de copia oculta? ¿La soléis utilizar?



Si Marta decidiese escribirle un e-mail a su amiga para aconsejarla el uso de la copia oculta, ¿Qué le escribiría? Podría comenzar:

"Me ha encantado el e-mail que me has enviado, la verdad es que era muy bonito…Pero he visto que aparecen todas las direcciones de correo electrónico de los amigos con los que has querido compartir este correo. Esto tiene algunos problemas y una muy fácil solución…"

(Se propone a los chicos y chicas que continúen la historia comentando algunos problemas y la solución).

4. CHATS.

Hoy Javier se ha metido en un foro donde se comenta su serie de televisión favorita. Mientras la comentaban, ha conocido a un usuario de este foro, "la perla", y le ha parecido muy simpático. Se han dado los correos personales para intentar conocerse mejor y han pensado en enviarse fotos personales…

1. ¿Crees que Javier está mostrando una actitud segura?

2. ¿Qué le dirías si estuvieses en su lugar?

3. ¿Creéis que es seguro intercambiar información personal con un "amigo virtual"?

Lo importante siempre es mantener una actitud segura, y en caso de dudas nunca facilitar información personal. En caso de que os veáis forzados o sintáis que es una situación extraña lo mejor es avisar a un adulto que os pueda ayudar.