

SEGURIDAD DE LOS USUARIOS ACTIVIDAD 1: CONSCIENTIZACIÓN

| | |
|-------------------------|--|
| Título de la actividad: | El uso seguro de mi email |
| Habilidad: | Seguridad de los usuarios |
| Medio: | Internet (Correo electrónico) |
| Sección: | Primaria alta |
| Tiempo: | 30 minutos |
| Objetivo: | El alumno conocerá qué es y cuál el propósito del correo electrónico, así como las principales medidas de seguridad en su uso. |
| Habilidades: | Juicio crítico, identidad personal, alfabetización digital. |



Introducción

El correo electrónico se llama así porque funciona de una forma similar a la del servicio postal.

Es un servicio gratuito por el puedes enviar y recibir mensajes de manera instantánea a través del internet, incluyendo fotografías o archivos de todo tipo.

A modo de introducción el docente puede proyectar este video con el fin de que los alumnos puedan entender cómo funciona el correo electrónico.

Video: https://youtu.be/ni_w00FkcNY

Una vez, ya conociendo cómo funciona el correo, es también muy importante que conozcan ciertas medidas de seguridad básicas en el uso de internet, que los ayudarán a minimizar los posibles riesgos a los que se puedan enfrentar, como son: virus, mensajes instantáneos, robo de identidad, extorsión, contenido no adecuado, cyberbullying, entre otros.

Es muy importante que los alumnos sepan que la edad mínima requerida para abrir una cuenta de correo o red social es de 13 años, por lo que papás y maestros deben fomentar el respeto de estas normas, explicándoles que es para su bien y por su seguridad.

Sin embargo, los docentes podemos irles preparando en estas edades para que tengan los conocimientos básicos de seguridad y estén listos para cuando puedan empezar a utilizar todas las aplicaciones y servicios que se pueden encontrar en internet.

Algunas de las medidas de seguridad básica son:

- *El poner filtros parentales en cada dispositivo les ayudará a que sus papás puedan conocer a qué sitios entran, el tiempo y con quién platican, recuerden que todo es por su propia seguridad y ellos mejor que nadie, sabrán orientarles en caso de que tengan alguna duda.*
- *Configuren los controles de seguridad y privacidad en cada una de las aplicaciones que usen.*
- *Vigilen por donde navegan. Entren sólo a páginas conocidas y confiables.*
- *No publiquen fotos o videos personales, no den información personal ni datos sensibles, sólo acepten contactos que conozcan en persona y avisen si detectan una conducta de acoso en Internet.*
- *No participen en chats o conversaciones online con otras personas, incluso si creen que sus interlocutores son niños también.*
- *No confíen en todos los emails, sobre todo los de enlaces o archivos que pidan descargarse, de cualquier aplicación que les llame la atención y tampoco de la publicidad que promete regalos o aquella que es muy llamativa e incita a entrar.*
- *Configuren contraseñas seguras y utilicen contraseñas diferentes para cada servicio. No las compartan con nadie, excepto con sus papás porque es por su propia seguridad.*

Material

- *Hoja de actividad (Alumno)*
- *Lápices y plumas*
- *Internet*
- *Video: https://youtu.be/ni_w00FkcNY*



Descripción

1. *El docente explicará con sus palabras la introducción al tema.*
2. *Proyectará el video propuesto.*
3. *Repartirá al alumno la hoja de actividades.*
4. *Explicará las instrucciones de la hoja de actividades.*
5. *Con todo lo visto, se dará una retroalimentación final con la participación de los alumnos.*

Reflexión

El correo electrónico te sirve para comunicarte con tu familia, amigos y profesores en todo el mundo. Recuerda que para utilizar de manera segura y efectiva el correo electrónico debes tomar en cuenta las siguientes medidas de seguridad: <https://www.segu-kids.org/menores/correo.html>

SEGURIDAD DE LOS USUARIOS ACTIVIDAD 1: CONSCIENTIZACIÓN



Título de la actividad:

El uso seguro de mi email

Objetivo:

Conoceré qué es y cuál el propósito del correo electrónico, así, como las principales medidas de seguridad en su uso.

Instrucciones

Resuelve la siguiente sopa de letras con los elementos del correo electrónico.

Dirección Correo electrónico Google Yahoo Mensaje Privacidad Mail Seguridad



A P R I V A C I D A D K L O P Ñ F X C V B M
 D I R E C C I O N I O L T F J L M A I L S E
 J Y I P D W S F D E L Ñ O P D S N B A G U N
 Z A Q S E G U R I D A D L P Ñ T D C X Q P S
 K H E W Q E R W W D I O S M G O O G L E Z A
 C O U P Ñ S A E D F G H L O P D F H V C N J
 C O R R E O E L E C T R O N I C O E N T O E
 R W I O P C S F T U W P U I O P F E Y V J L

Reflexión

El correo electrónico te sirve para comunicarte con tu familia, amigos y profesores en todo el mundo. Recuerda que para utilizar de manera segura y efectiva el correo electrónico debes tomar en cuenta las siguientes medidas de seguridad: <https://www.segu-kids.org/menores/correo.html>

SEGURIDAD DE LOS USUARIOS ACTIVIDAD 2: ANÁLISIS

| | |
|-------------------------|---|
| Título de la actividad: | El uso seguro de mi email |
| Habilidad: | Seguridad de los usuarios |
| Medio: | Internet (Correo electrónico) |
| Sección: | Primaria alta |
| Tiempo: | 30 minutos |
| Objetivo: | El alumno conocerá los elementos de un correo electrónico, así como algunas recomendaciones de seguridad para saber si un correo es spam. |
| Habilidades: | Juicio crítico, identidad personal, alfabetización digital, privacidad. |



Introducción

A modo de introducción se sugiere el siguiente video.

<https://youtu.be/31aTz2kfJDg>

Cuando ingresas a tu correo electrónico, notarás que de lado izquierdo se encuentra el panel de opciones que te permitirá ingresar a las carpetas de: bandeja de entrada, mensajes enviados, borradores, spam o correo no deseado y eliminados o papelera.

- **Bandeja de entrada.** Es un espacio en el que puedes ver los mensajes que te han llegado y los datos de su remitente: título o asunto y la fecha que se envió el mensaje.
- **Enviados.** Son los mensajes que si se enviaron a su destinatario de manera adecuada.
- **Borradores.** Son los mensajes que no se han enviado, y que puedes editar para enviarlos posteriormente.
- **Spam.** Se llama spam, correo basura o mensajes basura, generalmente son mensajes no solicitados o de remitente no conocido (correo anónimo).
- **Eliminados.** Son los mensajes borrados.

Es importante además como forma de proteger nuestra identidad y para no caer en algún ciber riesgo, saber detectar un correo spam, algunas formas de detectarlas son las siguientes:

(Texto recuperado de:

<https://www.redeszone.net/2018/01/30/descubre-5-formas-detectar-correo-electronico-spam/>)

- **El Remitente no corresponde con el servicio que envía el correo** Primero hay que observar la dirección desde la que se ha enviado el mensaje. Tal y como ya hemos dicho, en la mayoría de las ocasiones, los ciberdelincuentes utilizan la imagen de un servicio conocido para engañar a los usuarios. Si nos encontramos con una dirección así, por ejemplo: «soporte.netflix@xxxxxxxx.com, donde las X se sustituyen por el servicio genérico de hosting empleado, ese sería un ejemplo de dirección falsa.

• Gramática con fallos

Muchos ciberdelincuentes reaprovechan el mensaje para diferentes localizaciones y utilizan traductores, o ellos mismo lo realizan, lo más probable es que nos encontremos con faltas de ortografía o incoherencias gramaticales.

• URLs falsas camufladas en hipervínculos

En este caso se informa al usuario de un problema con la cuenta de un servicio y se le invita a acceder a la página web para iniciar sesión. En estos casos, los ciberdelincuentes nunca dejan al descubierto la dirección URL de la página, ya que no se encuentra en el dominio del servicio cuya imagen ha sido utilizada en el mensaje spam. Si el usuario se siente tentado de acceder, debe confirmar que la URL pertenece al servicio. De no ser así, no se debe introducir nunca información en el formulario. La finalidad de este no es otra que recopilar la información, enviada a servidores propiedad de los ciberdelincuentes.

• Archivos adjuntos que no son lo que parecen

En muchas ocasiones, sobre todo si se quiere instalar malware en el equipo del usuario, los ciberdelincuentes adjuntan documentos que a priori son Word o PDF comprimidos. Sin embargo, no hay que ser iluso en estas situaciones, si cuando realicemos la descompresión del archivo lo que aparece es un .exe, la acción siguiente a realizar será el borrado del mismo y del correo.

• Correo de un servicio que no utilizado o no contratado

Es el más evidente. Si recibes un mensaje reclamando una cantidad o adjuntando un documento de un servicio que no utilizas, lo más probable es que se trate de una estafa enviada de forma masiva.

Estas son algunas herramientas para saber cuándo un correo puede ser spam y, por lo tanto, lo mejor sería borrarlo.

Evaluación: Observación y participación de los alumnos

Material

- Computadora con internet (en caso de no contar con ella, el docente deberá orientarles para que contesten las actividades, fijarse muy bien en las historietas y en los ejemplos).
- Hoja de actividad (alumno)
- Lápices y plumas
- Video: <https://youtu.be/31aTz2kfJDg>



Descripción

1. *Explicar a los alumnos la introducción.*
2. *Investiga y escribe cinco correos electrónicos o nombres de dominio que sean falsos y otros 5 que sean confiables.*
3. *Platiquen con sus compañeros, cómo fue que identificaron esos correos o sitios de dominio.*
4. *El docente dará una reflexión al respecto*

Reflexión

Toma en cuenta que algunos mensajes pueden contener virus que afectan el rendimiento de tu computadora y hasta podrían robar tus datos personales. Por eso es importante analizar los mensajes que llegan, antes de abrirlos, para evitar caer en algún ciber riesgo.

SEGURIDAD DE LOS USUARIOS

ACTIVIDAD 2: ANÁLISIS



Título de la actividad:

Todos quieren comunicarse

Objetivo:

El alumno conocerá los elementos de un correo electrónico, así como tips de seguridad para saber si un correo es spam.

Instrucciones

Investiga y escribe cinco correos electrónicos o nombres de dominio que sean falsos y otros 5 que sean confiables. Fíjate en el ejemplo.

- Platica con tus compañeros, cómo fue que identificaron esos correos o sitios de dominio.

| CONFIABLES | SPAM |
|--|-------------------------------------|
| <i>marcial@conparticipacion.com.mx</i> | <i>http://www.bbva.mx/ganadores</i> |
| | |
| | |
| | |
| | |

Reflexión

Toma en cuenta que algunos mensajes pueden contener virus que afectan el rendimiento de tu computadora y hasta podrían robar tus datos personales. Por eso es importante analizar los mensajes que llegan, antes de abrirlos, para evitar caer en algún ciber riesgo.

SEGURIDAD DE LOS USUARIOS

ACTIVIDAD 3: REFLEXIÓN

| | |
|-------------------------|---|
| Título de la actividad: | El uso seguro de mi email |
| Habilidad: | Seguridad de los usuarios |
| Medio: | Internet (Correo electrónico) |
| Sección: | Primaria alta |
| Tiempo: | 30 minutos |
| Objetivo: | El alumno reconocerá cuáles son los principales riesgos en el correo electrónico. |
| Habilidades: | Juicio crítico, seguridad de los usuarios, empatía digital, identi- |



Introducción

A manera de introducción, el docente pedirá la participación de los alumnos para leer la siguiente historieta, se recomienda que se imprimen las imágenes tamaño póster para que todos lo alcancen a ver, o bien, descargadas para proyectarlas y que todos las puedan ver.

Evaluación: Observación y participación de los alumnos



PELIGROS DEL CORREO ELECTRÓNICO (I)

AL CONECTARNOS A INTERNET, ENTRAMOS A UN ENTORNO EN EL QUE NOS EXPONEMOS A UNA SERIE DE RIESGOS O PELIGROS.

TRAMPAS QUE NOS TIENDEN DESCONOCIDOS CON EL OBJETIVO DE ROBARNOS INFORMACIÓN O DINERO.

LO PRIMERO QUE DEBEMOS COMPRENDER ES QUE HAY DOS TIPOS PRINCIPALES DE AMENAZAS: AQUELLAS EN LAS QUE SE USAN SOBRE TODO ELEMENTOS TÉCNICOS Y AQUELLAS EN LAS QUE SE USA SOBRE TODO INGENIERÍA SOCIAL.

LA MAYORÍA DE VECES, AMBOS TIPOS DE AMENAZAS SE COMBINAN, COMO CUANDO SE UTILIZA UNA TÁCTICA DE INGENIERÍA SOCIAL PARA INFECTAR NUESTRA COMPUTADORA CON UN VIRUS.

SI QUIERES SABER CÓMO GANAR EN EL VIDEOJUEGO, DALE CLIC A ESTA LIGA

PARA DEFENDERNOS DE LOS ELEMENTOS TÉCNICOS EMPLEAMOS HERRAMIENTAS TÉCNICAS, COMO LOS ANTIVIRUS. PERO PARA DEFENDERNOS DE LA INGENIERÍA SOCIAL DEBEMOS SER SIEMPRE CUIDADOSOS Y USAR NUESTRO SENTIDO COMÚN.

EN INFORMÁTICA, LA INGENIERÍA SOCIAL ES UNA PRÁCTICA QUE INTENTA, POR MEDIO DE TODO TIPO DE ARTIMAÑANAS, QUE DESVELEMOS INFORMACIÓN PRIVADA O INCLUSO QUE REALICEMOS ACCIONES PERJUDICIALES PARA NOSOTROS MISMOS.

HECHA ESTA DIFERENCIACIÓN, VAMOS A VER AHORA UNA PEQUEÑA LISTA DE LAS AMENAZAS MÁS COMUNES QUE PUEDEN LLEGAR A NUESTRA BANDEJA ENTRADA.

UN EJEMPLO DE INGENIERÍA SOCIAL ES ENVIARNOS UN CORREO ELECTRÓNICO EN EL QUE LOS DELINCUENTES SE HACEN PASAR POR NUESTRO BANCO Y NOS PIDEN NUESTRA CONTRASEÑA.

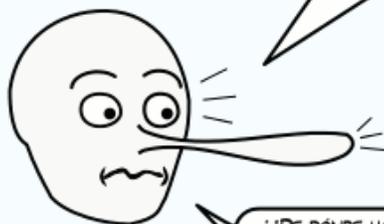


PELIGROS DEL CORREO ELECTRÓNICO (II)



HOAXES O BULOS

UN HOAX O BULO ES SIMPLEMENTE UNA INFORMACIÓN FALSA, POR LO GENERAL UNA NOTICIA. EN ESPAÑOL, SE SUELE UTILIZAR EL TERMINO INGLÉS, HOAX, PARA REFERIRSE A LOS BULOS QUE SE TRANSMITEN ESPECIFICAMENTE POR MEDIO DE INTERNET.



¿DE DÓNDE HA SALIDO ESTO SI YO NI TENGO NARIZ?!

LOS BULOS NO SON ALGO PARTICULAR DE INTERNET, SINO QUE PUEDEN TRANSMITIRSE TAMBIÉN POR OTROS MEDIOS. SIN EMBARGO, LA PROPIA NATURALEZA DE LA RED HA HECHO QUE SEA EN ELLA DONDE PROLIFEREN CON MÁS FACILIDAD.



EL PROPÓSITO DE UN HOAX NO SUELE SER ECONÓMICO, AL MENOS DIRECTAMENTE. LAS INTENCIONES DETRÁS DE QUIEN LO GENERA PUEDEN SER MUY VARIADAS. E INCLUSO PUEDE SER FRUTO ÚNICAMENTE DE LA IGNORANCIA, ACEPTANDO HECHOS COMO CIERTOS CUANDO SÓLO SON LEYENDAS URBANAS.



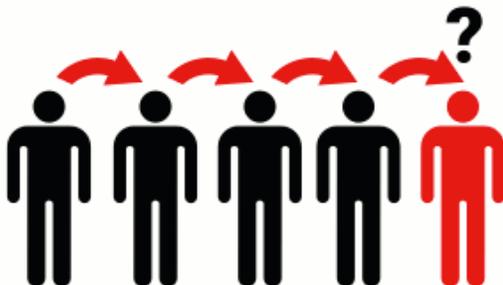
SIN EMBARGO, YA QUE UN HOAX TIENE COMO CARACTERÍSTICA PRINCIPAL SER MUY LLAMATIVO, SE SUELE UTILIZAR PARA CAPTAR DIRECCIONES DE CORREO ELECTRÓNICO QUE LUEGO PERMITAN TRANSMITIR AMENAZAS MÁS PELIGROSAS.

Mensaje nuevo

Para amigo1@correo.com x amigo2@correo.com
amigo3@correo.com x amigo4@correo.com
amigo5@correo.com x amigo6@correo.com
amigo7@correo.com x amigo8@correo.com
amigo9@correo.com x amigo10@correo.com
amigo11@correo.com x amigo12@correo.com
amigo13@correo.com x amigo14@correo.com
amigo15@correo.com x amigo16@correo.com
amigo17@correo.com x amigo18@correo.com



EL EJEMPLO MÁS CLÁSICO DE HOAX SUELEN SER ESAS NOTICIAS DE QUE SE VAN A CERRAR SERVICIOS MUY POPULARES Y QUE CIRCULAN DE CORREO EN CORREO. O SUCESOS IMPACTANTES QUE LES HAN SUCEDIDO SIEMPRE AL AMIGO DE UN AMIGO; ES DECIR, LEYENDAS URBANAS.



CON LA POPULARIZACIÓN DE REDES SOCIALES, LOS BULOS FRUTO DE LA CREDULIDAD, DE LA MALICIA O HASTA CON OBJETIVOS DE MANIPULACIÓN SOCIAL SE HAN TRASLADADO A ELLAS. PERO ESO NO SIGNIFICA QUE NO SE CONTINÚE USANDO EL CORREO ELECTRÓNICO PARA DIFUNDIRLOS.



POR ELLO, DEBEMOS SIEMPRE ESTAR ALERTAS ANTE CUALQUIER HOAX QUE LLEGUE A NUESTRA BANDEJA DE ENTRADA Y NO CONTRIBUIR A DIFUNDIRLO.

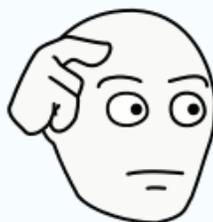


PELIGROS DEL CORREO ELECTRÓNICO (III)



SPAM

EL SPAM O CORREO BASURA SON MENSAJES NO DESEADOS Y NO SOLICITADOS, EN LA MAYORÍA DE LAS OCASIONES DE REMITENTE ANÓNIMO, DESCONOCIDO O DIRECTAMENTE FALSO.



GENERALMENTE SON DE CARÁCTER PUBLICITARIO, TRATANDO DE VENDER NOS TODO TIPO DE PRODUCTOS, MUCHOS (SI NO TODOS) DE DUDOSA PROCEDENCIA O DE DUDOSA EFECTIVIDAD.



LOS MENSAJES DE ESTE TIPO PUEDEN CONTENER TAMBIÉN ARCHIVOS ADJUNTOS QUE ESTÉN INFECTADOS CON SOFTWARE MALICIOSO, O INCLUIR ENLACES ENGAÑOSOS QUE NOS LLEVEN A DESCARGÁRNOSLO.



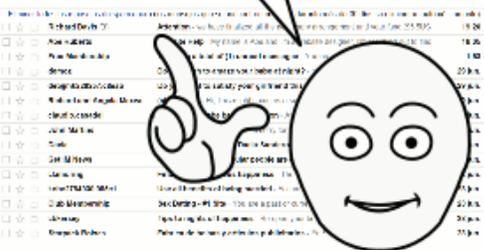
EL SPAM ADEMÁS TAMBIÉN ES EL VEHÍCULO DE OTRAS AMENAZAS, COMO LOS INTENTOS DE ESTAFA (SCAM) O DE PHISHING. DE ESTOS DOS TÉRMINOS HABLAREMOS EN LAS PÁGINAS SIGUIENTES.



NO RECIBIR SPAM EN UNA CUENTA DE CORREO ELECTRÓNICO ES PRÁCTICAMENTE IMPOSIBLE. SEGÚN LOS REPORTES REALIZADOS POR EL M³AAWG, EL 90% DE LOS MENSAJES ENVIADOS POR CORREO EN TODO EL MUNDO DURANTE 2014 FUERON DE SPAM. POR ESO ES IMPORTANTE ESTAR ALERTA FRENTE A MENSAJES SOSPECHOSOS.



HOY DÍA, LOS PRINCIPALES PROVEEDORES DE CORREO DETECTAN DE MANERA EFECTIVA EL SPAM, AUNQUE SUS FILTROS DISTAN DE SER PERFECTOS, POR LO QUE NO ES RARO QUE SE NOS CUELE ALGUNO EN NUESTRA BANDEJA DE ENTRADA. DE AHÍ QUE NUNCA SEA POSIBLE BAJAR LA GUARDIA.



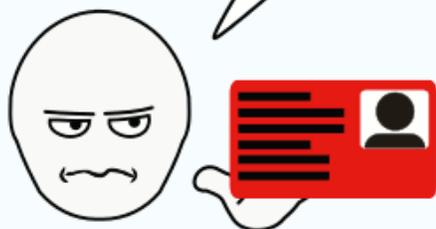


PELIGROS DEL CORREO ELECTRÓNICO (IV)



PHISING

LAS TÁCTICAS DE INGENIERÍA SOCIAL SUELEN BASARSE EN LA SUPLANTACIÓN DE IDENTIDAD O EN EL OFRECIMIENTO DE INFORMACIÓN FALSA.



LA TÁCTICA DE SUPLANTACIÓN MÁS UTILIZADA ES LA QUE SE CONOCE COMO PHISING. EN ELLA, SE NOS PIDE QUE INTRODUCAMOS INFORMACIÓN EN LA QUE PARECE SER UNA PÁGINA WEB COMPLETAMENTE LEGÍTIMA, COMO LA DE NUESTRO BANCO, Y A LA QUE LLEGAMOS A TRAVÉS DE UN ENLACE RECIBIDO POR CORREO.



CON LA POPULARIDAD DE REDES SOCIALES, HAN APARECIDO TAMBIÉN INTENTOS DE PHISING EN LOS QUE SE NOS INSTA A REVELAR NUESTRAS CONTRASEÑAS DE ESTAS REDES. Y, COMO NO, EL CLÁSICO DE PEDIRNOS LA CONTRASEÑA DE NUESTRO CORREO ELECTRÓNICO.

Necesitamos que nos haga llegar su contraseña para poner el marcha la adaptación al nuevo sistema de pago...



LA SUPLANTACIÓN DE IDENTIDAD SIEMPRE SUELE DARSE HACIÉNDOSE PASAR POR UN SERVICIO O UN SITIO WEB CONOCIDO DEL QUE SEAMOS USUARIOS. PERO TAMBIÉN PUEDE DARSE LA SUPLANTACIÓN DE UNO DE NUESTROS CONTACTOS.



ALGUIEN QUE CONOZCAMOS PUEDE TENER SU COMPUTADOR COMPROMETIDO O SU CUENTA DE CORREO. ENTONCES, ES POSIBLE QUE RECIBAMOS MENSAJES DESDE SU DIRECCIÓN CON CONTENIDO MALICIOSO.

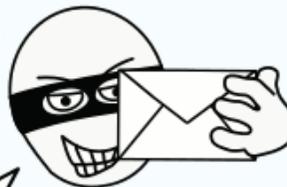
¿PARA QUÉ QUERÍAS LA CONTRASEÑA QUE ME PEDISTE EL OTRO DÍA?

YO NO TE PEDÍ NADA.

¡¿QUÉ?!



LAS DIRECCIONES DE CORREO TAMBIÉN SE PUEDEN SUPLANTAR, DE MANERA QUE RECIBAMOS UN MENSAJE DESDE UNA DIRECCIÓN DE ALGUIEN QUE CONOZCAMOS PERO QUE EN REALIDAD NO PROVIENE DE ALLÍ.



ESTOS DOS ÚLTIMOS MÉTODOS NO SON TAN UTILIZADOS DE MANERA GENERALIZADA, LO CUAL NO QUIERE DECIR QUE NO DEBAMOS ESTAR ALERTA ANTE ELLOS.

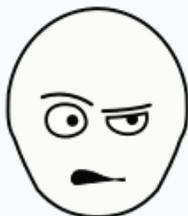


PELIGROS DEL CORREO ELECTRÓNICO (VI)

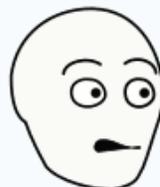


MALWARE

COMO HEMOS DICHO, EL MALWARE SON PROGRAMAS QUE ALTERAN EL COMPORTAMIENTO DE NUESTRA COMPUTADORA DE UNA MANERA QUE NOS RESULTA PERJUDICIAL.



EN OCASIONES, SE LE SUELE DENOMINAR "VIRUS" AL MALWARE DE MANERA GENERAL, PERO ESTO ES ERRÓNEO. LOS VIRUS SON TAN SÓLO UN TIPO DE MALWARE. TODOS LOS VIRUS SON MALWARE, PERO NO TODO EL MALWARE SON VIRUS.



CADA TIPO TIENE UN OBJETIVO DIFERENTE, COMO PUEDE SER ROBAR INFORMACIÓN O DESTRUIRLA.

EN BASE A SU MODO DE FUNCIONAMIENTO Y A LOS OBJETIVOS QUE PERSIGUE, PODEMOS CLASIFICAR EL MALWARE EN LOS SIGUIENTES TIPOS.



| | | |
|---|---|--|
| VIRUS  | GUSANOS  | BACKDOORS  |
| ROOTKITS  | TROYANOS  | SPYWARE  |
| KEYLOGGERS  | ADWARE  | BOTNETS  |

ALGUNOS DE LOS OBJETIVOS MÁS COMUNES QUE SE PERSIGUEN CON EL MALWARE SON:



CREAR EQUIPOS ZOMBIS PARA ENVIAR SPAM, REALIZAR ATAQUES DDOS A SITIOS WEB, ETC.



MOSTRAR PUBLICIDAD DE FORMA INTRUSIVA O REDIRECCIONAR VISITAS HACIA ELLA.



DESTRUIR DATOS O BLOQUEARLOS HASTA QUE SE REALICE UN PAGO.



ROBAR INFORMACIÓN SENSIBLE COMO CONTRASEÑAS, TARJETAS DE CRÉDITO, ETC.



INTERCEPTAR COMUNICACIONES.



RECOPILAR INFORMACIÓN DE NUESTRAS ACTIVIDADES EN INTERNET.



Material

- Historietas impresas o descargadas para proyectar
- Hoja de actividad (para el alumno)
- Lápiz o pluma
- Colores

Descripción

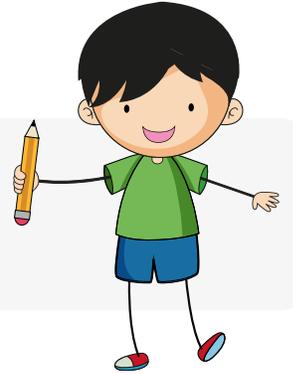
1. *El docente pedirá a los alumnos que lean las historietas que se les presenta, para explicarles los distintos riesgos en el correo electrónico. Una vez que terminen que leerlas, el docente dará una retroalimentación sobre lo leído.*
2. *Repartir la hoja de actividades y realizar la actividad según las instrucciones especificadas, utilizando varios colores. En este caso, en algunas preguntas puede haber dos o más respuestas correctas, deberán reflexionar cuál sería la mejor solución para no caer en esos riesgos.*
3. *Realizar una reflexión entre todos, sobre los riesgos en el correo electrónico.*

Reflexión

El conocer los riesgos y amenazas más frecuentes que se dan en Internet, te permitirá saber actuar de manera correcta para prevenirlos o hacerles frente. Recuerda siempre consultar a tus papás antes de abrir algún correo que te parezca extraño.

SEGURIDAD DE LOS USUARIOS

ACTIVIDAD 3: REFLEXIÓN



Título de la actividad:

El uso seguro de mi email

Objetivo:

Conoceré cuáles son los principales riesgos del correo electrónico y cómo actuar, en cualquier caso.

Instrucciones

Relacionas las columnas



Si un desconocido te contacta en las redes sociales y te sugiere que se conozcan...

Consulta a tus padres

¿Qué haces si una persona te intimida por medio de un mensaje?

Elimínalo de tus contactos

Si recibes mails de una persona que no conoces...

No lo abras

Si una persona te pide tu contraseña de email o alguna información personal...

No respondas

Si te llega un mensaje en donde te dice que ganaste algo...

Le envío mis datos

Lo reporto a las autoridades

Reflexión

El conocer los riesgos y amenazas más frecuentes que se dan en Internet, te permitirá saber actuar de manera correcta para prevenirlos o hacerles frente. Recuerda siempre consultar a tus papás antes de abrir algún correo que te parezca extraño.

SEGURIDAD DE LOS USUARIOS ACTIVIDAD 4: ACCIÓN

| | |
|-------------------------|---|
| Título de la actividad: | El uso seguro de mi email |
| Habilidad: | Seguridad de los usuarios |
| Medio: | Internet (Correo electrónico) |
| Sección: | Primaria alta |
| Tiempo: | 30 minutos |
| Objetivo: | El alumno escribirá un correo electrónico a un compañero de clase, con los elementos ya vistos en las actividades anteriores. |
| Habilidades: | Juicio crítico, seguridad de los usuarios, empatía digital, identidad personal, alfabetización digital. |



Introducción

A manera de introducción, para tener una buena práctica al enviar un correo electrónico.

Es importante recordarles a los alumnos que para poder tener una cuenta de correo electrónico se requiere que tengan 13 años, son embargo se les pedirá que escriban un correo en su hoja de actividades para que practiquen estos buenos hábitos a la hora de mandar un correo.

Evaluación: Observación y participación de los alumnos



BUENAS PRÁCTICAS ADICIONALES (I)



INCLUYE UNA FIRMA EN TUS MENSAJES

MUCHOS SERVICIOS DE CORREO Y PROGRAMAS CLIENTE PERMITEN INSERTAR DE MANERA AUTOMÁTICA UN PEQUEÑO TEXTO AL FINAL DE CADA MENSAJE QUE ENVÍES.

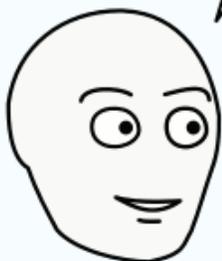
Hola:

No te olvides de enviarme la información que me prometiste.

Un saludo.

Gregorio Casillas
Mi [blog](#) - Mi [Facebook](#) - Mi [Twitter](#)

"No backup, no plan and nothing to loose"



UNA FIRMA ES UNA MANERA MUY ÚTIL DE DAR A CONOCER TUS PROYECTOS O TU MANERA DE PENSAR.

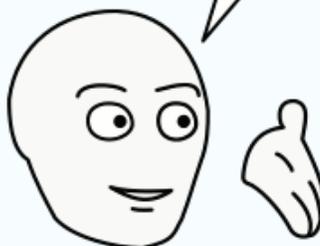
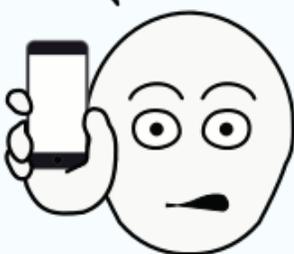
INCLUYE UNA FIRMA ESPECÍFICA PARA CUANDO CONTESTES DESDE EL TELÉFONO MÓVIL



LAS APLICACIONES PARA REVISAR EL CORREO DESDE TELÉFONOS INTELIGENTES SUELEN CONTAR CON UNA OPCIÓN PARA AÑADIR UNA FIRMA ESPECÍFICA EN LOS MENSAJES ENVIADOS DESDE ELLAS. SÍ, ES EL CLÁSICO "ENVIADO DESDE MI IPHONE" O "ENVIADO DESDE MI TELÉFONO CON ANDROID".

ESTO TIENE SU SENTIDO MÁS ALLÁ DE LA MERA PROMOCIÓN, PUES SIRVE PARA INDICAR QUE EL MENSAJE SE HA ENVIADO DESDE UN DISPOSITIVO MÓVIL, LO QUE EXPLICA QUE NO ESTÉ BIEN REDACTADO, TENGA ALGUNAS FALTAS O QUE INCLUSO SEA MUY BREVE O SECO.

SI NO QUIERES UTILIZAR LA FIRMA QUE AÑADE LA APLICACIÓN POR DEFECTO, CREA LA TUYA PROPIA. PERO RECUERDA QUE DEBE DEJAR CLARO QUE ESTÁS ENVIANDO EL CORREO DESDE UN DISPOSITIVO MÓVIL, NO DESDE EL ESCRITORIO.





BUENAS PRÁCTICAS ADICIONALES (II)



NO ENVÍES NI REENVÍES DE MANERA INDISCRIMINADA

CUANDO ALGO NOS GUSTA, TENDEMOS A COMPARTIRLO, PERO PUEDE SER QUE NO A TODAS LAS PERSONAS DE LAS QUE TIENES LA DIRECCIÓN LES GUSTE ESE CHISTECITO QUE TANTO TE HA HECHO REÍR.

TEN CUIDADO ADEMÁS DE QUE, SI HACES UN REENVÍO, NO LO HAGAS A TODOS LOS CONTACTOS DE TU LISTA.

PARA ESTAS COSAS, USA MEJOR FACEBOOK, TWITTER, GOOGLE+ O CUALQUIER OTRA RED SOCIAL O APLICACIÓN DE MENSAJERÍA.

NO ENVÍES CORREOS A MUCHAS DIRECCIONES AL MISMO TIEMPO



TODO PROVEEDOR DE CORREO TIENE SU LÍMITE DE DIRECCIONES A LAS QUE PUEDES ENVIAR UN MISMO MENSAJE.

SI LO SUPERAS, EMPEZARÁS A SER SOSPECHOSO DE SPAM (CORREO NO DESEADO) Y TU CUENTA PODRÍA SER CANCELADA O DESHABILITADA POR UN TIEMPO.

EL LÍMITE SUELE VARIAR, PERO SUPERAR LAS 100 DIRECCIONES NO ES ALGO MUY RECOMENDABLE.



BUENAS PRÁCTICAS ADICIONALES (III)



NO ENVÍES CORREOS GENERALIZADOS COMO PROMOCIÓN

SI QUIERES DAR A CONOCER TU PRODUCTO, TU PROYECTO, TU WEB O LO QUE SEA A UNA SERIE DE PERSONAS, NUNCA ESCRIBAS UN CORREO GENERAL.

LA GENTE MUESTRA RECHAZO ANTE LOS CORREOS INDISCRIMINADOS, SOBRE TODO AQUELLOS CON COSAS COMO "QUERIDO/A AMIGO/A" O "QUERID@ AMIG@".

ESCRIBE SIEMPRE UNO PERSONALIZADO PARA CADA PERSONA A LA QUE SE LO VAS A ENVIAR.

DAN IMPRESIÓN DE PEREZA Y DESINTERÉS, COMO SI EL REMITENTE QUISIERA ALGO DEL DESTINATARIO SIN IMPORTARLE REALMENTE QUIÉN ES O QUÉ HACE.

REVISA PERIÓDICAMENTE EL SPAM



LOS PROVEEDORES DE CORREO CUENTAN CON UN SISTEMA DE FILTRADO DE SPAM QUE CADA DÍA ES MÁS EFICIENTE. PERO TODAVÍA DISTA DE SER PERFECTO.

POR ESO ES IMPORTANTE REVISAR CADA CIERTO TIEMPO LA CARPETA O SECCIÓN DE SPAM POR SI HA IDO A PARAR ALLÍ UN MENSAJE DE FORMA INCORRECTA. CON HACERLO UNA VEZ AL MES, SUELE SER SUFICIENTE.

TEN EN CUENTA DE QUE EL SPAM SUELE ELIMINARSE DE FORMA AUTOMÁTICA PRECISAMENTE CADA MES Y QUE LAS DIRECCIONES DE MENSAJES QUE HAYAN TERMINADO ALLÍ SERÁN SIEMPRE CATALOGADAS COMO SPAM A MENOS QUE SEÑALEMOS LO CONTRARIO.

Chats
Todos
Spam (419)
Papelera
Trabajo
Administrar etiquetas
Crear etiqueta nueva

Material

- Historietas impresas o descargadas para proyectar
- Hojas de actividades
- Lápiz
- Colores

Descripción

1. *El docente pedirá a los alumnos que lean las historietas que se les presenta, para explicarles las buenas prácticas a la hora de redactar un correo electrónico.*
Además de la información de las historietas, el docente puede leer la siguiente liga para poder orientar de mejor manera a sus alumnos.
<https://www.ionos.mx/digitalguide/correo-electronico/e-mail-marketing/como-escribir-un-correo-formal/>
Una vez que terminen que leerlas, el docente dará una retroalimentación sobre lo leído.
2. *Repartir la hoja de actividades y realizar la actividad según las instrucciones especificadas.*
3. *Realizar una reflexión entre todos, sobre lo visto a lo largo de estas 4 sesiones sobre seguridad en el correo electrónico y lo importante de escribir bien un correo electrónico, no sólo desde el punto de vista de seguridad, si no también en cuanto a la forma, la ortografía y redacción.*

Reflexión

El correo electrónico es un medio de comunicación eficaz que te permite tener contacto con personas en todo el mundo. Recuerda las reglas básicas para mandar y recibir correos y así evitarás los riesgos que se pueden presentar.

SEGURIDAD DE LOS USUARIOS

ACTIVIDAD 4: ACCIÓN



Título de la actividad: El uso seguro de mi email
Objetivo: Escribiré un correo electrónico a un compañero de clase, con algún mensaje de amistad

Instrucciones

Con todos los elementos adquiridos para crear un correo electrónico, enviarás un mensaje a un compañero con el tema de amistad.

Mensaje nuevo — ↗ ✕

Para | Cc CCO

Asunto

↶ ↷ Sans Serif ▾ ↕ ▾ **B** *I* U A ▾ ▮ ▮ ▮ ▮ ▮ ▮ ▾

Enviar ▾ A 📎 🔗 😊 📎 📎 📎 ⋮ 🗑️

Reflexión

El correo electrónico es un medio de comunicación eficaz que te permite tener contacto con personas en todo el mundo. Recuerda las reglas básicas para mandar y recibir correos y así evitarás los riesgos