MANUAL SOBRE
SEGURIDAD EN INTERNET

VIRUS

¿Qué son?	Consecuencias
Los *virus* informáticos son programas que se propagan ocultos dentro de otro programa, correo electrónico, página web, o fichero, alterando el funcionamiento del equipo al que infectan.	Los *virus* alteran el correcto funcionamiento del PC. Entre otras cosas, pueden llegar a eliminar información del disco duro, o hacer que el ordenador se reinicie cada pocos minutos, o incluso abrir puertos de comunicaciones permitiendo que un intruso controle el ordenador de forma remota.

¿Cómo evitarlos?

- Instala un software de antivirus y tenlo actualizado, ya que todos los días salen nuevos *virus*

  Euskaltel proporciona a través de su producto ***"Antivirus de Correo"*** *un servicio que protege a tu ordenador de los virus que puedan entrar o salir a través del correo electrónico, sin necesidad de comprar ni instalar ningún programa antivirus y sin tener que preocuparte de las actualizaciones. Euskaltel lo hace por ti.*

  Para solicitarlo sólo tienes que llamar al ***1717*** *o acercarte a tu* ***Punto de Venta Euskaltel*** *más cercano*

- Nunca ejecutes un fichero adjunto en un correo electrónico si no estás seguro de quién te lo envía y su contenido.
- Sé especialmente precavido cuando descargues software de sitios dudosos.
- No aceptes nunca archivos que no hayas solicitado cuando estés en el chat (IRC) o grupos de noticias (news).
- Realiza copias de seguridad de la información valiosa cada cierto tiempo.

INTRUSIONES

¿Qué son?	Consecuencias
Las *intrusiones* se producen cuando alguien no deseado accede al ordenador de forma remota.	El intruso puede llegar a obtener información confidencial o a ocultar su identidad, lanzando acciones desde nuestro ordenador. Por ejemplo, el atacante puede llegar a introducir programas en nuestro ordenador que graben las pulsaciones del teclado y así obtener datos confidenciales como contraseñas.

¿Cómo evitarlos?

- Envía tu correo electrónico con autenticación. Esto evitará que los spammers hagan envíos masivos de correos electrónicos desde tu PC y que en Internet se te identifique como spammer y por tanto tu IP sea metida en listas negras. Estas listas negras son consultadas por algunos operadores, y aquellos que las consultan limitan el envío desde esas direcciones, por lo que dejarás de poder enviar correo a conocidos que tienen como proveedor de Internet dichos operadores. Más tarde tendrás que dedicar tiempo a gestionar la reclamación para hacer que tu IP se elimine de la lista negra. Puedes ver como configurar el envío de correo autenticado en: http://www.euskaltel.com/web/home_attclipartic.jsp?elegido=1&linea=Internet
- Instala un firewall o cortafuegos. Los firewalls son las herramientas más utilizadas para que sólo tenga acceso a tu ordenador quien tú quieras.
- Elimina del PC los protocolos de red que no sean necesarios para conectarse a Internet. Es decir, todos excepto el protocolo TCP/IP. Esto se realiza desde Inicio -> Panel de Control -> Red, seleccionando el protocolo a eliminar y pulsando Quitar
- No compartas archivos o impresoras a través del protocolo TCP/IP. Para ello desde Inicio -> Panel de Control -> Red , elige el protocolo TCP/IP y pulsa en Propiedades. Luego selecciona la pestaña Enlaces y desmarca Compartir Impresoras y Archivos para Redes Microsoft
- Deshabilita NetBIOS sobre TCP/IP para evitar que el intruso pueda ver los recursos que estás compartiendo en el PC. Para deshabilitarlo volvemos a elegir el protocolo TCP/IP, pulsamos Propiedades y seleccionamos la pestaña NetBIOS, ahí se desmarca la opción NetBIOS. Si no se permite desmarcarlo es que ya está deshabilitado
- Siempre que un programa te solicite la conexión a Internet, y ante la duda de qué es lo que quiere hacer, lo mejor es denegar este permiso. Si después te percatas de que algo que necesitabas del programa que estás utilizando no funciona, puedes entonces permitir el acceso.
- No proporciones ni tus nombres de usuario, ni las claves de ninguno de tus servicios de Internet (acceso, correo electrónico, FTP, etc.). Tampoco divulgues tu IP fija si es que la tienes
- Si utilizas conexiones con tarifa plana (ADSL, cable o RTB), apaga el PC cuando no uses la conexión. Es más seguro y ahorrarás energía.

SPAM

¿Qué son?	Consecuencias
Son e-mails no solicitados, que normalmente buscar de vender algo	Pérdida de tiempo para el usuario ya que tiene que molestarse en identificarlos y borrarlos para que no le ocupen espacio en su buzón

¿Cómo evitarlos?

- Si publicas notas en alguna web o grupo de noticias, utiliza una cuenta de correo alternativa.
- De la misma forma que no das tu número de teléfono a extraños, tampoco lo hagas con tu correo electrónico. Siempre que en una web te soliciten un registro, lee despacio las condiciones y asegúrate de lo que harán con esa información.
- Si recibes muchos e-mails no deseados del mismo remitente, bloquéale con los filtros de tu programa de correo, para hacer que esos mensajes sean rechazados o enviados directamente a la papelera.
- Rompe las cadenas de mensajes, muchas veces se ocultan detrás de buenas causas, pero en realidad pretenden hacerse con direcciones de correo electrónico.
- Nunca respondas a un spam. Es una señal inequívoca de que tu cuenta está activa. Igualmente, no visites una página o pulses sobre una imagen que aparezca en un correo de este tipo.
- Si no quieres recibir spam, cuando envíes un mensaje a las news escribe algún identificador que haga imposible que pueda ser recogido de forma automática por programas informáticos (nombre@QUITAESTOdominio.com, nombre@dominioESTONOVALE.com) , tanto en la dirección de correo de la cabecera del mensaje como en la firma. Hazlo siempre a la derecha de la arroba y nunca en el nombre.
- Informa a tu proveedor de Internet de aquellas personas o empresas que envían spam.

DIALERS

¿Qué son?

Los *dialers* se utilizan para redirigir, de forma maliciosa, las conexiones mientras se navega por Internet. Su objetivo es colgar la conexión telefónica que se está utilizando en ese momento y establecer otra, marcando otro número de teléfono cuyo coste es mucho más elevado.

Consecuencias

Se puede llegar a recibir una factura telefónica de importe desorbitado.

Los dialers solamente pueden causar problemas en accesos de banda estrecha ya que los accesos de banda ancha no requieren marcar ningún número de teléfono.

¿Cómo evitarlos?

- Puedes solicitarnos a través del 1717 la desconexión de los números que aplican tarifas especiales. Así evitarás cualquier problema.
- Instala un programa anti-dialer. Este programa configura una lista de números permitidos (lista blanca), de modo que el programa sólo permite la conexión con alguno de esos números y rechaza el resto. Puedes descargar un anti-dialer gratuito en: http://www.hispasec.com/software/checkdialer/index.html
- Comprueba que no se haya modificado el Acceso Telefónico a Redes que utilizas habitualmente para tus conexiones de manera que, cada vez que sea ejecutado, el número marcado no sea el correspondiente al proveedor de servicios de Internet, sino el de un número de tarifa especial.
- Comprueba que no se haya creado un nuevo "Acceso Telefónico a Redes" que, además, es el que el ordenador va a usar siempre por defecto para conectarse a Internet.
- Ten cuidado con algunas páginas, sobre todo las de contenido para adultos, que te piden que instales un nuevo Acceso Telefónico a Redes con un número de teléfono de pago incrementado, o incluso lo crean sin que te des cuenta con un dialer.
- Ante todo, sé muy precavido. La forma en que los dialers se ofrecen es engañosa. En demasiadas ocasiones las páginas webs que cargan estos programas se anuncian como de contenidos gratuitos.
- La publicidad puede jugarte malas pasadas. Muchas veces pulsar sobre uno de los banners que anuncian ciertos contenidos (sobre todo juegos y contenidos para adultos) es suficiente para que se ejecute el programa que carga el dialer.

BUGS

¿Qué son?	Consecuencias
Los *bugs* son errores del software	Pueden hacer que el ordenador no funcione correctamente (aparición de ficheros extraños, lentitud en su funcionamiento, que el equipo se reinicie sin motivo, etc.) o permitir que un intruso pueda colarse en él.

¿Cómo evitarlos?

- Actualiza regularmente el software de tu ordenador a las últimas versiones (sistema operativo, navegador, u otras aplicaciones)

  Microsoft ha creado algunas herramientas para solucionar el problema de los bugs en sus sistemas operativos Windows. Uno de ellos es Windows Update. Desde la página de Windows Update (http://windowsupdate.microsoft.com), Microsoft te ofrece automáticamente una selección de las actualizaciones más recientes disponibles para su sistema operativo, programas y hardware de tu equipo.

- Realiza copias de seguridad o backups de forma sistemática para prevenir posibles pérdidas de información.