MANUAL DE NAVEGACIÓN

1) ACTUALIZAR O NAVEGADOR:

Cando utilizamos o navegador (Mozilla, Chrome, Explorer...) estamos abrindo a porta de entrada a Internet.

Moitos virus están fabricados para actuar sobre o navegador e poder controlar as súas funcións: opcións de procura, redirixir a propia procura e, en definitiva, obter información, controlala e manipulala.

A resposta das empresas responsables dos navegadores consiste en actualizalos para responder a tales ataques e resolver os problemas. En consecuencia se non actualizamos o navegador podemos ser vítimas de tales ataques.

Hai casos nos que non chega coa actualización do navegador e necesitamos desinstalalo e volvelo instalar de novo.

2) ABRIR OU DESCARGAR UN ARQUIVO DESCOÑECIDO:

Os arquivos executables de orixe descoñecido que poidamos recibir no noso correo electrónico case sempre son virus (a súa extensión é "exe.")

O máis sensato é non descargalos nin executalos no ordenador.

3) USAR O MESMO CONTRASINAL PARA ACCEDER A VARIAS CONTAS:

Moitas persoas empregan o mesmo contrasinal para acceder ao correo electrónico, Facebook, Tuenti, Twiter, Instagram, etc. É certo que resulta máis sinxelo lembrar un contrasinal (password) para varias contas, mais a un *hacker* que obteña o noso único contrasinal, resultaralle moi fácil acceder ao resto de contas, para utilizalas sen a nosa autorización.

O mellor e máis seguro é ter un contrasinal para cada conta.

4) NON BORRAR O HISTORIAL DE NAVEGACIÓN:

Cando accedemos a internet, deixamos unha pegada por cada páxina ou lugar ao que accedemos ou visitamos, que é o noso historial de navegación.

Tamén deixamos unha pegada nas cookies que se almacenan no noso disco duro.

Podemos evitalo utilizando a "navegación privada" e borrando as cookies almacenadas no noso equipo.

5) TER UN ANTIVIRUS QUE NON ESTÁ ACTUALIZADO:

O mesmo que os navegadores, os antivirus renóvanse continuamente para facer fronte ás novas ameazas.

As actualizacións teñen unha duración anual ou mensual e o seu custo pode variar dependendo do número de equipos nos que se pode utilizar.

Cómpre, pois, ter un antivirus actualizado, ou utilizar un sistema operativo (como por exemplo o "Ubuntu") máis seguro.

6) PROTOCOLO HTTPS PÁXINAS WEB:

As páxinas nas que operamos con compras ou transaccións comerciais adoitan estar cifradas e para iso utilizan o protocolo HTTPS. Isto sabémolo fixándonos na barra de enderezos do noso navegador. Se o nome da páxina comeza por "https", é segura.

Exemplos:

https://www.google.es/searchclient=ubuntu&channel=fs&q=XUNTA+GALICIA&i

https://bancaelectronica.abanca.com/

(Se facemos unha operación bancaria e a entidade bancaria non ten ese protocolo https, é posible que sexa unha web clonada ou falsificada para substraer os nosos datos e cartos. Esta práctica denominase "phising". O ***phishing*** *é unha técnica de captación ilícita de datos persoais (principalmente relacionados con claves para o acceso a servizos bancarios e financeiros) a través de correos electrónicos ou páxinas web que imitan/copian a imaxe ou aparencia dunha entidade bancaria/financeira (ou calquera outro tipo de empresa de recoñecido prestixio).*

En términos máis coloquiais, podemos entender o phishing como "pesca de datos",

A técnica do phishing utiliza o correo electrónico para poñerse en contacto cos usuarios, utilizando mensaxes que imitan, case á perfección, o formato, linguaxe e a imaxe das entidades bancarias/financeiras, e que sempre inclúen unha petición final na que solicitan aos usuarios a "confirmación" de determinados datos persoais, alegando distintos motivos: problemas técnicos, cambio de política de seguridade, posible fraude etc...

Estas mensaxes de correo electrónico sempre inclúen ligazóns que conducen aparentemente ás páxinas web oficiais das citadas entidades pero que, en realidade, remiten a "páxinas web trucadas" que imitan ou copian case á perfección a páxina web da entidade financeira, sendo a súa finalidade principal captar datos dos usuarios.

Dada a confianza que os usuarios teñen depositada nas entidades das que son clientes, e por descoñecemento ou simplemente ante a

incerteza e temor creados, acceden ás devanditas páxinas web trucadas, onde o defraudador ou delincuente informático, obtén os datos persoais ou claves de acceso persoais.

É a partir deste momento onde empeza a fraude:

- *Utilización do número de tarxeta e data de caducidade para compras por Internet (comercio electrónico).*
- *Realización de transferencias bancarias non consentidas nin autorizadas.*
- *Retirada de efectivo en caixeiros con duplicados das tarxetas.)*

7) CONFIAR NO SPAM:

O spam é o correo electrónico non desexado, e adoita multitude de formas: ofertas fabulosas, notificacións da obtención dun premio, ofertas de emprego atractivas... Na práctica, o spam é o envío repetido dunha gran cantidade de mensaxes de correo electrónico para distribuír información inútil, propaganda e unha variedade de propostas. Supón un desperdicio de recursos técnicos e de tempo de atención dos usuarios. As persoas e sistemas que os envían colleitan estes enderezos con programas que os buscan automaticamente en páxinas web, guías, directorios, chats e grupos de novas. O mellor é eliminalos e non confiar en ofertas dubidosas e milagreiras.

8) FACER COMPRAS OU ACCEDER A DATOS BANCARIOS DESDE UNHA REDE WIFI PÚBLICA:

Nunca debemos acceder á nosa conta bancaria ou facer compras por Internet desde un ordenador dun cibercafé ou cun aparello (portátil, móbil, tablet...) da nosa propiedade, pero conectado a unha rede WIFI pública. Os ordenadores públicos (dun cibercafé, dunha biblioteca,...) son obxectivos favoritos dos delincuentes informáticos, que poden instalar programas que detectan as claves secretas que tecleamos neles. Os puntos Wifi públicos poden estar controlados de forma que calquera información que enviemos a través da rede (computador,teléfono..) poida ser roubada por un *hacker*[1].

9) NON CONTROLAR A NOSA INFORMACIÓN PERSONAL NAS REDES SOCIAIS:

A nosa privacidade sempre debe ser o máis restritiva posible, e moito máis se usamos as redes sociais. Debemos evitar que todo o mundo acceda ao noso perfil e aos nosos datos persoais (idade, fotos, comentarios, etc). Só aquelas persoas que coñecemos e os nosos amigos deben ter acceso aos mesmos. Unha configuración inaxeitada da nosa privacidade na rede social pode facilitar que outros nos vixíen sen o noso permiso coa intención de utilizar esa infomación para prexudicarnos.

Temos que evitar a publicación de fotografías comprometidas, pois despois de publicalas perdemos todo control sobre elas, o cal pode causarnos no futuro multitude de problemas, tanto laborais como sociais.

IES ILLA DE ONS

[1] *Hacker*: Cando falamos de seguridade informática, referímonos con este termo a entradas non autorizadas nos nosos aparellos de acceso a Internet.

Consellos para navegar con seguridade pola rede

IES Illa de Ons

Rúa A Pedra 51 36930 - Bueu
☏986324130 🖷986324331
ies.illa.ons@edu.xunta.es
http://www.edu.xunta.es/centros/iesillaons/