# TEMA 4

# SEGURIDADE E PRIVACIDADE EN EQUIPOS E REDES

# Backdoors

Un backdoor é un programa que se introduce no computador de maneira encuberta, aparentando ser inofensivo. Unha vez é executado, establece unha "porta traseira" a través da cal é posible controlar o computador afectado. Isto permite realizar no mesmo accións que poden comprometer a confidencialidade do usuario ou dificultar o seu traballo.

As accións permitidas polos “backdoors” poden resultar moi prexudiciais. Entre elas atópanse a eliminación de ficheiros ou a destrución da información do disco duro. Ademais, poden capturar e reenviar datos confidenciais a unha dirección externa ou abrir portos de comunicacións, permitindo que un posible intruso controle o noso computador de forma remota.

# Troianos

Un troiano ou cabalo de Troia é un programa que se diferencia dos virus en que non se reproduce infectando outros ficheiros. Tampouco se propaga facendo copias de si mesmo como fan os vermes.

O seu nome deriva do parecido na súa forma de actuar cos astutos gregos da mitoloxía: chegan ao computador como un programa aparentemente inofensivo. Con todo, ao executalo instalará no noso computador un segundo programa, o troiano.

Os efectos dos troianos poden ser moi perigosos. Permiten realizar intrusións ou ataques contra o computador afectado, realizando accións tales como capturar todos os textos introducidos mediante o teclado ou rexistrar os contrasinais introducidos polo usuario.

Os troianos de porta traseira poden facerse pasar por programas lexítimos para enganar aos usuarios e que os executen. Noutros casos (cada vez máis habituais), os usuarios permiten a entrada do troiano no computador sen sabelo ao facer clic nunha ligazón recibida nunha mensaxe de correo non desexado ou ao visitar unha páxina web maliciosa.

Ao executarse, o troiano se autoinclúe na rutina de inicio do computador e, a partir dese momento, pode vixiar o equipo ata que o usuario se conecta a Internet. Unha vez que o computador está conectado a Internet, a persoa que enviou o troiano pode realizar moitas accións como, por exemplo, executar programas no equipo infectado, acceder a arquivos persoais, modificar e cargar arquivos, rexistrar as pulsacións no teclado ou enviar mensaxes de correo non desexado.

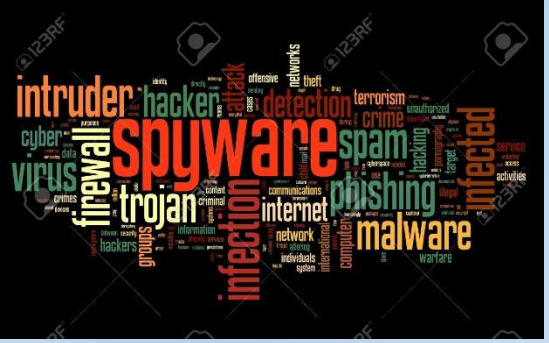
# Vermes

Os vermes son programas moi similares aos virus, xa que tamén se autoreplican e teñen efectos daniños para os computadores, pero diferéncianse en que non necesitan infectar outros ficheiros para reproducirse, en lugar de necesitar un programa ou arquivo portador.

Basicamente, os vermes limítanse a realizar copias de si mesmos, sen tocar nin danar ningún outro ficheiro, pero reprodúcense a tal velocidade que poden colapsar por saturación as redes nas que se infiltran. Principalmente esténdense a través do correo electrónico.

Os vermes de execución automática son programas maliciosos que abusan da función de autoexecución de Windows para executarse de forma automática ao conectar o dispositivo no que están almacenados a un computador. Estes adoitan distribuírse en unidades USB e infectan os equipos ao conectalas, instando aos usuarios a elixir entre escoitar música co reprodutor de medios predeterminado ou abrir o disco no Explorador de Windows.

Algúns vermes abren portas traseiras nos computadores que os ciberdelincuentes poden utilizar para facerse co control. Despois, os computadores poden utilizarse para enviar correo non desexado.




# Spyware

Os programas espía, tamén coñecidos como spyware, son aplicacións informáticas que recompilan datos sobre os hábitos de navegación, preferencias e gustos do usuario. Os datos recollidos son transmitidos aos propios fabricantes ou a terceiros non autorizados como anunciantes, ben directamente, ben despois de ser almacenados no computador. O spyware pode ser instalado solicitando previamente ou non o consentimento do usuario, así como con plena conciencia ou falta dela acerca da recompilación de datos e/ou do uso que se vai a realizar dos mesmos. Os programas espía, que se consideran como un tipo de troiano, consomen memoria e capacidade de procesamiento, o que pode afectar á velocidade dos equipos ou facer que se bloqueen.

O antispyware é unha tecnoloxía de seguridade que axuda a protexer a un equipo contra spyware e outro software potencialmente non desexado. Este software axuda a reducir os efectos causados polo spyware incluíndo o lento rendemento do equipo, xanelas de mensaxes emerxentes e cambios non desexados en configuracións de Internet. Tamén protexe contra os programas que rastrexan a información sobre hábitos de consumo e navegación, ou peor aínda, contrasinais e outros datos sensibles.

Ao momento de seleccionar un antispyware, debe de incluír as seguintes características xerais:

- Bloqueo antes de que o spyware se descargue ou instale. É moito máis fácil previr que limpar
- Cerciorarse de que o antispyware estea actualizado.
- Executar exploracións automáticas da computadora en días e horas concretas.
- Capacidade para poder restaurar ou reverter compoñentes borrados inadvertidamente.


# Adware e Dialers

ADWARE

Adware é unha palabra inglesa que nace da contracción das palabras Advertising Software, é dicir, programas que mostran anuncios, empregando calquera tipo de medio: xanelas emerxentes, banners, cambios na páxina de inicio ou de procura do navegador, etc. O adware pode ser instalado co consentimento do usuario e á súa plena conciencia, pero en ocasións non é así. O mesmo ocorre co coñecemento ou falta do mesmo acerca das súas funcións.

DIALERS

"Dialer" é un programa que, sen o consentimento do usuario, colga a conexión telefónica que permite o acceso a Internet e que se está utilizando nese momento, e establece outra, marcando un número de teléfono de tarificación especial. Isto suporá un notable aumento do importe na factura telefónica. Os "dialers" NON funcionan con conexións ADSL e/ou cable xa que este tipo de conexións non realiza marcado para unha conexión telefónica. Por esa razón, agora xa se ven estes programas moi raramente.

# Bulos


Os bulos son declaracións falsas ou sen corroborar que tentan enganar ou estafar aos usuarios. O obxectivo dos bulos pode ser conseguir diñeiro, instalar programas maliciosos ou consumir ancho de banda (facendo que os usuarios reenvíen mensaxes do bulo). Os bulos por correo electrónico poden:

- Advertir sobre programas maliciosos novos moi perigosos e difíciles de detectar.
- Suxerir que non se lean mensaxes con determinados asuntos porque supostamente conteñen programas maliciosos.
- Afirmar que unha empresa de software importante, un provedor de Internet ou unha institución gobernamental publicaron a advertencia.
- Afirmar que o programa malicioso fai cousas pouco probables.
- Incitar a reenviar a advertencia.
- Afirmar que, ao facer clic en “gústame" nalgún comentario ou usuario de Facebook, pódese gañar diñeiro, facer donativos ou conseguir premios gratis.

Cando moitos usuarios reenvían este tipo de bulos, poden producirse inundacións do correo electrónico que sobrecargan os servidores. Os bulos tamén poden distraer e entorpecer os esforzos por solucionar ameazas reais. A mellor defensa contra os bulos é a formación dos usuarios. Tamén resulta útil buscar información en Internet sobre todo aquilo que pareza un bulo. Hai varios tipos de bulos coñecidos, como os *“hoaxes”* (avisos de falsos virus) e os *“jokes”* (bromas).

# Bugs e buratos de seguridade

Nos inicios da computación, os computadores non contiñan os circuítos integrados con millóns de transistores de hoxe en día. Os ordenadores tiñas centos de cables e arandelas magnetizadas, que necesitaban varias habitacións para despregarse. Un destes computadores históricos era o ENIAC. En certa ocasión, este xigantesco equipo comezou a fallar e non lograba executar ningún programa. O problema persistía durante tanto tempo, que os programadores decidiron revisar o sistema por completo, aínda que tal misión puidese levarlles semanas enteiras de traballo. Por fin, entre unha maraña de cables, un deles atopou o cadáver dun insecto que cortocircuitaba a memoria. Ao retirala todo volveu funcionar. Desde entón os erros de programación coñécense como "*bugs*" (insecto en inglés).

Todo o software que tes instalado no teu computador pode ter erros; á fin e ao cabo, detrás dun programa informático hai un equipo de persoas encargadas de desenvolvelo e estas, en ocasións, tamén se equivocan. Canto maior sexa o nivel de complexidade das tarefas que executa o programa, maiores son as súas posibilidades de ter erros. Os *bugs* máis preocupantes son aqueles que afectan o sistema operativo do computador, posto que é o elemento común a todas as actividades que realizamos co equipo. Un *bug* pode ter efectos desconcertantes, como que un ficheiro non poida imprimirse, ou erros graves que afecten á seguridade do teu PC. Cando isto é así, convértense en verdadeiros buratos polos que un intruso pode coarse.

Os buratos de seguridade diferéncianse dos *bugs* correntes en que non se adoitan detectar, xa que non están asociados a disfuncións do software. Con todo, si son buscados de forma intensiva por moitos programadores, co obxecto de invadir computadores alleos. A única forma verdadeiramente fiable de detectar un burato de seguridade en calquera programa é executalo en todas as condicións posibles. Pero, como é lóxico, as combinacións son tan numerosas que iso sería como buscar agullas nunha palleira.

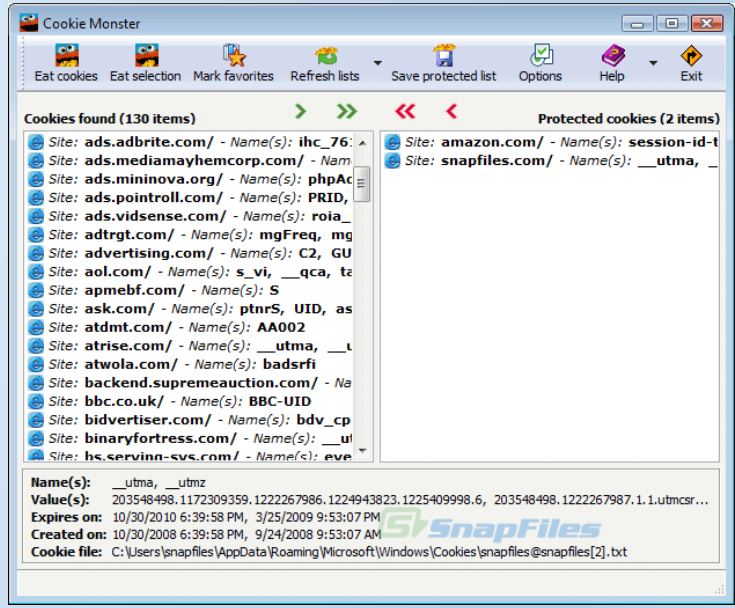
O habitual é que as novas versións dun software teñan erros que se van corrixindo a medida que se van detectando. Esta é a explicación á necesidade de ir xerando novas versións ou, simplemente, de parches específicos para resolver os problemas creados polos *bugs*. O mellor que podes facer cando te atopes cun erro ao que non atopas explicación, é poñerte en contacto co fabricante do software que estás a utilizar e comunicarllo, xa que podes estar en presenza dun *bug*.

# Cookies

As cookies son pequenos ficheiros de texto que se gardan no noso navegador a petición do servidor, ás veces sen o coñecemento nin o consentimento dos usuarios. A información que conteñen é relativa á páxina que estivemos visitando, como pode ser o noso nome de usuario e clave ao acceder a ela, algunhas preferencias, as veces que habemos ir, etc. Ao ser un ficheiro de texto, non é potencialmente perigoso xa que como tal non é executable (non pode introducir nin virus, nin executar programas, etc), só é iso, texto.

Aínda que nun principio as cookies eran utilizadas polo servidor para axudarlle a soportar a carga do seu sistema, agora é moi utilizada como fonte de información sobre os nosos hábitos ao navegar, por exemplo polos anunciantes, para levar un mellor control do noso "perfil". Cando falamos do noso perfil, non falamos do noso nome, teléfono, etc.. (a non ser que llo facilitemos, claro) senón de que é o que nos interesa, que é o que non lle prestamos atención, etc.

Outro problema das cookies é precisamente que se almacenan no teu disco duro, polo que se alguén ten acceso a el (fisicamente ou través dunha rede) podería coñecer eses datos e utilizalos (por exemplo, se hai usuarios e contrasinais). Os navegadores modernos teñen a posibilidade de desactivar a vontade as cookies (en Opcións de seguridade).




# Correo electrónico

O correo electrónico é un dos servizos máis utilizados en Internet. Cando se envía un correo electrónico normal (non encriptado), o que estamos a enviar, utilizando o símil do correo ordinario, é unha postal, non unha carta que está pechada e hai que romper o sobre para lela, e é perfectamente visible para calquera. Se o texto da mensaxe ten formato “html”, pode ter problemas como a inclusión de códigos ou enlaces maliciosos.

Unha práctica moi corrente é achegar arquivos ás mensaxes de correo electrónico. Estes arquivos poden ser de calquera tipo (follas de cálculo, documentos, imaxes, programas, etc..) e son a principal vía polas que o malware infecta os nosos computadores. É moi recomendable NON executar os arquivos adxuntos co clásico dobre click, xa que iso executaría o posible malware.

As regras ou filtros de correo son utilidades do cliente de correo electrónico (Webmail, Outlook, Thunderbird, etc.) para organizar as mensaxes recibidas. Permiten analizar os correos electrónicos recibidos e realizar accións automáticas en función de certas condicións personalizadas. A modo de exemplo, pódense establecer condicións como  que a dirección do remitente ou do destino conteñan certo texto, e marcar como lida a mensaxe.

Algúns consellos máis sobre correo electrónico poderían ser:

- Se non coñece ao remitente dunha mensaxe non solicitada e non lle interesa o tema, elimíneo
- Utilice o campo CCO ao enviar unha mensaxe de correo electrónico a varias persoas á vez
- Non expoña en exceso a súa dirección de correo electrónico
- Separe o correo electrónico de traballo do persoal, utilice direccións diferentes
- Desactive a opción para recibir máis ofertas ou información

# Spam


O spam é o correo electrónico non solicitado, normalmente con contido publicitario, que se envía de forma masiva. Habitualmente as direccións do remitente son falsas ou foron secuestradas a usuarios reais, o Asunto é moi rechamante e os temas son publicitarios e agresivos (produtos milagre, gañar cartos doadamente, etc.). Boa parte del está en inglés pero xa comeza a abundar en español.

O spam é un fenómeno que vai en aumento día a día, e representa unha elevada porcentaxe do tráfico de correo electrónico total. A medida que xorden novas solucións e tecnoloxías máis efectivas para loitar contra o spam, os spammers (usuarios maliciosos que se dedican profesionalmente a enviar spam) vólvense á súa vez máis sofisticados, e modifican as súas técnicas con obxecto de evitar as nosas contramedidas.

O correo non desexado adoita ser rendible. Os remitentes de correo non desexado poden enviar millóns de mensaxes nunha soa campaña por moi pouco diñeiro. Con só 1 destinatario de entre 10.000 que realice unha compra, poden obter beneficios. Podemos sinalar os seguintes factores como importantes no correo non desexado:

- O correo non desexado utilízase a miúdo para distribuír programas maliciosos.
- Os remitentes de correo non desexado adoitan utilizar computadores alleos para enviar spam.
- O correo non desexado, do mesmo xeito que os bulos e os virus por correo electrónico, utilizan ancho de banda e ocupan espazo nas bases de datos.
- Por outra banda, poden confundir mensaxes importantes con correo non desexado e pasalos por alto ou eliminalos.
- O correo non desexado fai perder o tempo ás persoas. Os usuarios sen protección anti-spam teñen que comprobar que mensaxes son correo non desexado e eliminalos.
- Ademais, na actualidade, os creadores de spam están a aproveitar a popularidade da mensaxería instantánea e redes sociais como Facebook e Twitter para sortear os filtros de correo non desexado e enganar aos usuarios para que revelen información delicada e financeira.

# Portos de comunicación

Un PC necesita, para comunicarse co resto de computadores conectados a Internet, ter unha dirección electrónica e poder identificarse ante os demais. Esa dirección electrónica é a dirección IP. Pero iso non é suficiente, xa que en Internet pódense utilizar moitos e diversos servizos e é necesario poder diferencialos. A forma de facelo é mediante os portos (non hai que confundilos cos portos de E/S).

Imaxinemos un edificio de oficinas: este ten unha porta de entrada ao edificio (que sería o IP) e moitas oficinas que dan servizos (os portos de comunicacións). Iso lévanos a que a dirección completa dunha oficina vén dada pola dirección postal e o número da oficina. No caso de Internet vén dado pola dirección IP e polo número de porto. Así por exemplo, un servidor web escoita as peticións que lle fan polo porto 80, un servidor FTP faino polo porto 21, etcétera. É dicir, os portos son os puntos de enganche para cada conexión de rede que realizas.

Para que un atacante consiga controlar o teu computador, primeiramente tivo que entrar nel por unha porta aberta, é dicir, por un porto de comunicacións que non estaba convenientemente asegurado. Igual que na túa casa non deixas as xanelas e as portas abertas de par a par, no teu equipo debes ter coidado para evitar intrusións sempre que esteas conectado á Rede.

Existen mais de 65.000 portos diferentes usados para as conexións de Rede. Se no teu computador cóase a través do correo electrónico un virus capaz de abrir algún destes portos, o resultado é que a porta da túa casa quedará aberta. Podes estar seguro de que calquera porto aberto que ti non controles (en ocasións é posible que nin tan sequera saibas que existe) é unha invitación para que poidan fisgar no teu equipo, roubarche información confidencial e ocasionarche multitude de problemas.

Unha medida básica de seguridade é coñecer que portos ten o teu equipo, cales están abertos e por que o están. Entre estes últimos, ademais, debes ter en conta cales non estás a utilizar e os que poden ocasionar un problema de seguridade.

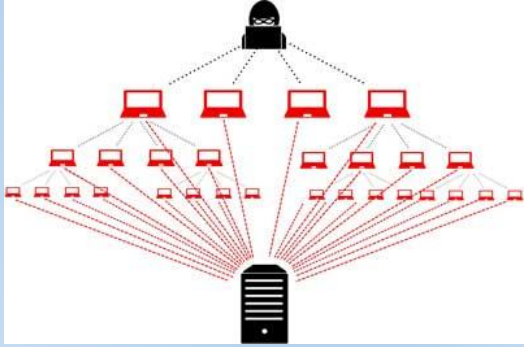
Existen dúas formas básicas de combater aos intrusos unha vez que xa solicitamos toda a información acerca dos portos. A primeira delas consiste en bloquear os portos, é dicir, pechar aqueles que non queiras utilizar. Outro método, moito máis efectivo, é pechalos todos e instalar un firewall ou cortalumes. Este programa só permite o tráfico con Internet que ti aceptes, facendo unha consulta cada vez que necesita abrir un porto para que algo salga ou entre no teu equipo.

# Redes de bots

As redes de bots son grupos de computadores infectados controlados de forma remota por un hacker. Unha vez que o software malicioso (bot) infecta un equipo, o agresor pode controlalo de forma remota por Internet. A partir dese momento, o equipo convértese nun zombi ás ordes do hacker sen que o usuario chegue a decatarse. Os grupos de equipos infectados desta maneira denomínanse redes de bots.

Os delincuentes poden compartir o control da rede de bots ou vender acceso á mesma para que outros poidan utilizala con fins maliciosos. Por exemplo, un creador de correo non desexado pode utilizar unha rede deste tipo para enviar spam. A maior parte do correo non desexado distribúese desta forma, xa que permite aos remitentes evitar ser detectados e sortear as listas negras nas que se puideron incluír os seus servidores. Ademais, posto que os donos dos computadores pagan polo acceso a Internet, reduce os custos. Os delincuentes tamén utilizan redes de bots para lanzar ataques distribuídos de denegación de servizo, ameaza que explicamos xusto a continuación.

# Ataque de denegación de servizo



Os ataques de denegación de servizo (DDoS, polas súas siglas en inglés) impiden que os usuarios accedan a un equipo ou un sitio web. Neste tipo de ataques, os delincuentes tentan sobrecargar ou bloquear un servizo para que os usuarios lexítimos non poidan utilizalo.

O tipo de ataque DDoS máis habitual é o utilizado para enviar a un computador máis tráfico do que pode recibir. Os ataques de denegación de servizo utilizan unha gran variedade de métodos, pero a inundación de servidores web con solicitudes desde redes de bots é o máis sinxelo e habitual. Non se rouban nin se secuestran datos, pero a interrupción do servizo pode resultar custosa para as empresas.


# Secuestro de DNS e Pharming

O sistema de nomes de dominios ou DNS é a guía telefónica de Internet e serve para que os equipos poidan traducir nomes de sitios web a direccións IP para poder comunicarse (vémolo no tema 5).

Os secuestros de DNS cambian a configuración dos equipos para que ignoren o DNS oficial ou utilicen un servidor de DNS controlado polos ciberdelincuentes, que redirixen a comunicación a sitios fraudulentos.

Este tipo de ataques adoita utilizarse para levar aos usuarios a páxinas de inicio falsas e outros servizos por Internet co fin de roubar credenciais, que non poidan actualizar os programas de protección, etc.

O pharming consiste en manipular as direccións DNS que utiliza o usuario, co obxectivo de enganarlle e conseguir que as páxinas que visite o usuario non sexan realmente as orixinais senón outro sitio de aparencia similar, coa finalidade de enganar aos usuarios para obter os seus nomes e contrasinais de acceso.

# Descarga automática e Rexistro de pulsacións

DESCARGA AUTOMÁTICA

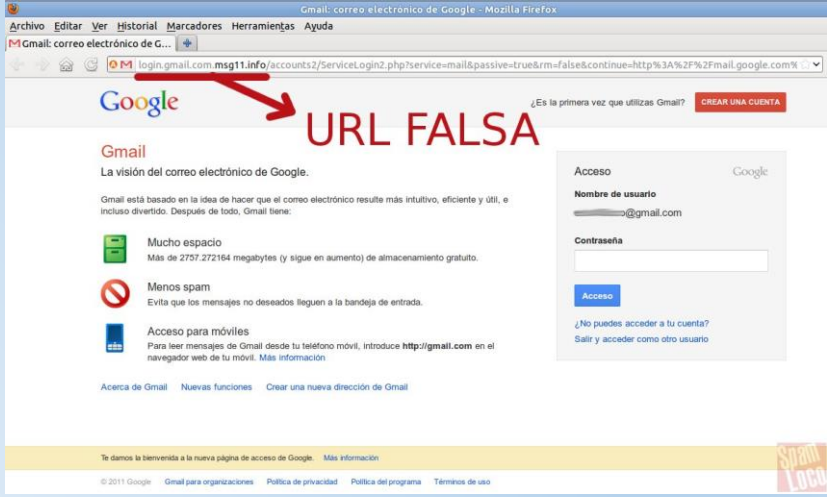
As descargas automáticas infectan os equipos con malware cando os usuarios simplemente visitan un sitio web malicioso, e prodúcense sen que os usuarios se decaten. O programa malicioso aproveita as vulnerabilidades do navegador (e os complementos) para infectar o equipo.

Os ciberdelincuentes atacan sitios web lexítimos continuamente para secuestralos e inxectar código malicioso nas páxinas. Así, cando os usuarios visitan ese sitio lexítimo (aínda que secuestrado), o código infectado cárgase no navegador, iniciando o ataque automático. Desta forma, os delincuentes poden infectar os equipos dos usuarios sen ter que enganarlles para que visiten un sitio web específico.

REXISTRO DE PULSACIÓNS

O rexistro de pulsacións é o proceso mediante o cal terceiros non autorizados gardan pulsacións no teclado dos usuarios de forma secreta. Os programas maliciosos adoitan utilizalo para roubar nomes de usuario, contrasinais, datos de tarxetas de crédito e outros datos delicados. Son habitualmente coñecidos como “keyloggers” e hainos en software e en hardware.

# Suplantación de identidade ou Phishing




A suplantación de identidades ou “phishing” é o proceso mediante o cal os ciberdelincuentes enganan aos usuarios para que revelen información delicada. Normalmente, a través dos timos de mensaxes de suplantación de identidades, os usuarios reciben unha mensaxe de correo electrónico que parece provir dunha institución de confianza, por exemplo: Bancos, Redes sociais (Facebook, Twitter), Xogos por Internet, Servizos en liña con acceso á información financeira do usuario, ou Departamentos da empresa do usuario. Esas mensaxes adoitan incluír un enlace que, ao ser pulsado, leva a páxinas web falsificadas. Desta maneira, o usuario, crendo estar nun sitio de toda confianza, introduce a información solicitada que, en realidade, vai parar a mans do estafador.

Habitualmente usan nomes de compañías xa existentes ou incluso dalgún empregado real, para transmitir confianza, e direccións web con aparencia correcta. Tamén xogan co factor medo, porque a xanela de oportunidade dos defraudadores é moi breve, por tanto, é fundamental para o defraudador o conseguir unha resposta inmediata por parte do usuario.

Algúns consellos para evitar os ataques de “phishing” poderían ser:

- Non pulsar en enlaces incluídas en mensaxes de correo electrónico. Mellor introduza a dirección do sitio web na barra do navegador e vaia á páxina correcta, ou utilice un marcador ou un favorito.
- Tampouco abra arquivos adxuntos que poidan traer esas mensaxes.
- Non responda a mensaxes de correo electrónico que soliciten información financeira persoal
- Preste atención ás mensaxes sospeitosas e notifique ás autoridades calquera actividade sospeitosa

# Loterías falsas e Scam

LOTERÍAS FALSAS

No falso premio de loterías, o usuario recibe un correo electrónico onde lle notifican que ten un premio de lotería. Se contesta a este correo, solicítanselle a continuación todos os datos bancarios para un falso ingreso do premio. Noutros casos, solicítaselle unha parte do premio que terá que envialo a un país para poder cobrar o premio completo. En todos os casos, o premio é falso.

SCAM

O Scam é a captación de persoas por medio de correos electrónicos, anuncios en web de traballo, chats, irc, etc... onde empresas ficticias ofrécenlle traballar comodamente desde casa e cobrando uns beneficios moi altos. Sen sabelo, a vítima esta blanqueando diñeiro obtido por medio do *phishing* (procedente de estafas bancarias). Algunhas características son:

- Sempre lle piden que teña ou abra unha conta bancaria.
- O seu traballo consiste en recibir transferencias bancarias á súa conta bancaria, sacar este diñeiro posteriormente para envialo a países estranxeiros por medio de empresas tipo Western Union, Money Gram.
- Frases para captar a victimas: Está vostede en paro e ten ganas de traballar? Quere obter un diñeiro extra? Quere traballar comodamente desde casa? Quere ter beneficios de forma rápida?
- Mándannos un contrato (falso) para facer mais crible a oferta.

Unha vez obtidos os datos da victima, se non colabora, será ameazada.

# Compras por Internet (I)

A especial dinámica comercial de Internet, onde non temos un contacto físico co vendedor, fai que realizar o pago poida ser orixe dunha fraude. Sempre que sexa posible é recomendable realizar as compras a través de empresas coñecidas ou algunha institución financeira de confianza. Comprobar os datos que elas mesmas nos ofrecen na súa páxina web e facer unha busqueda en Internet sobre esa compañía axudaranos a coñecer se existe algun problema con elas. As compras a través de páxinas de poxas son as que máis problemas poden ocasionarnos se non se seguen uns mínimos consellos de seguridade que elas mesmas nos proporcionan. Non se recomendan os pagos por transferencia instantánea entre persoas descoñecidas. Utiliza as formas de pago que che ofrezan maiores garantías.

NORMAS DE SEGURIDADE PARA ACCEDER Á BANCA E COMPRAS POR INTERNET

Non temos que baixar a garda en canto a "protexer" as nosas operacións bancarias de posibles manipulacións, de posibles roubos das nosas finanzas ou dos nosos datos, tal como facemos na vida normal. Vostede ha de tomar precaucións tal e como faría ao sacar diñeiro dun caixeiro automático ou ao pagar cunha tarxeta de crédito. Uns posibles consellos serían:

1.- Evitar no máximo posible acceder á túa Banca por internet ou levar a cabo transaccións financeiras en lugares públicos onde o acceso a Internet está dispoñible para moitas persoas, por exemplo Ciber-Cafés, Universidades, Colexios, Oficinas, redes wi-fi públicas, etc. Se se ve forzado a facelo, evite que haxa persoas moi preto e peche o navegador ao finalizar as súas operacións. Canto antes, cambie as claves de acceso de seguridade desde o seu computador persoal.

2.- Ter o seu navegador actualizado para ter os protocolos de seguridade en regra.

# Compras por Internet (II)

3.- Observar se a dirección comeza con https: en lugar de só http:

4.- O Banco NUNCA lle solicitará que informe das súas claves ou datos a través do correo electrónico.

5.- Garde as súas claves de acceso en segredo. Nunca as revele a ninguén nin as anote en lugares visibles ou de fácil acceso, como a pantalla, teclados, nin en documentos moi visibles.

6.- Use claves aleatorias e cambie as súas claves periodicamente e sempre que intúa que poden ser coñecidas por outras persoas ou foron utilizadas en lugares públicos.

7.- Se realiza algunha operación monetaria garde unha copia ou imprima a información, a maioría de web bancarias teñen esta función.

8.- Cando estea a acceder á Banca por Internet non desatenda as súas operacións distraéndose con outras cousas, é mellor bloquear o computador ou apagalo.

9.- Peche a sesión cando termine de operar coa súa oficina virtual.

10.- Borre o caché do seu navegador ao finalizar a sesión.

11.- Instale algún programa antivirus no seu equipo e mantéñao actualizado.

12.- Sempre que teña dúbidas da seguridade, pregunte na súa sucursal bancaria, informaranlle e aconsellarán detalladamente de como acceder á súa "oficina virtual".

# Ransomware

Un ransomware (do inglés ransom, ‘rescate’) é un tipo de programa informático malintencionado que cifra algúns arquivos inutilizando en certo xeito o dispositivo e coaccionando ao usuario a pagar o rescate, para coñecer a contraseña que descifra de novo eses arquivos. Normalmente un ransomware transmítese como un troiano ou como un verme, infectando o sistema operativo, por exemplo, cun arquivo descargado ou explotando unha vulnerabilidade do software.

Fixéronse populares en Rusia e o seu uso creceu internacionalmente en xuño do 2013. WanaCrypt0r, tamén coñecido como "WannaCry", é un ransomware "activo" que apareceu o 12 de maio de 2017. Provocou o cifrado de datos en máis de 75.000 ordenadores por todo o mundo, afectando, entre outros países, a Rusia, Reino Unido, Estados Unidos, España, China, Italia e Taiwán. Os sistemas operativos máis vulnerables ante el son Windows Vista, Windows 7, Windows Server 2012, Windows 10 e Windows Server 2016.


# ANTIVIRUS

Os antivirus informáticos son programas cuxa finalidade consiste na prevención, procura, detección, bloqueo e/ou eliminación de calquera programa maligno. Estes programas inclúen virus, vermes, spyware, ou calquera outra das ameazas que acabamos de ver, que se executan sen a autorización do usuario e que poden consumir recursos ou memoria e até eliminar información. Un antivirus pode pertencer a un ou varios dos seguintes tipos:

ANTIVIRUS PREVENTORES: caracterízanse por anticiparse á infección, previndoa, permanecendo na memoria da computadora.

ANTIVIRUS IDENTIFICADORES OU DE PATRÓN: identifican determinados programas infecciosos que afectan o sistema, rastrexando secuencias de códigos específicos vinculados cos devanditos virus.

ANTIVIRUS DESCONTAMINADORES: pretenden descontaminar un sistema que foi infectado, a través da eliminación de programas malignos.

ANTISPYWARE: ten o obxectivo de descubrir e descartar aqueles programas espías que se sitúan na computadora de maneira oculta.

ANTIPOP-UPS: ten como finalidade impedir que se executen as xanelas pop-ups ou emerxentes, é dicir a aquelas xanelas que xorden repentinamente sen que o usuario o decida.

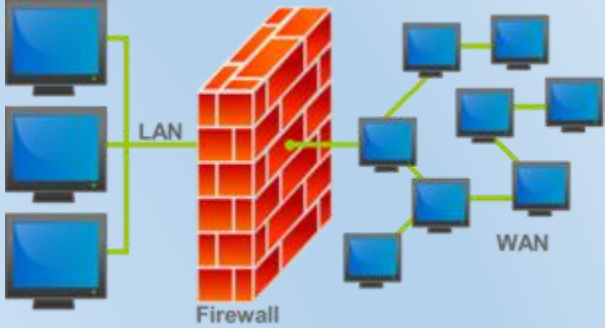
ANTISPAM: teñen o obxectivo de detectar o spam e eliminalo de forma automática.

PROGRAMAS DE VACINA: estes antivirus traballan engadíndolle códigos aos ficheiros executables para que se autochequeen no momento da execución, e así detectar vírus.

RESIDENTES: estes antivirus analizan os programas desde o momento en que o usuario os executa e atópanse situados na memoria.

ANTIVIRUS EN LIÑA: son utilizados para pescudar se hai virus no ordenador, e non deben ser instalados xa que se executan desde Internet. Só se activan cando se entra na súa web.

# CORTALUMES (I)




Un cortalumes é unha parte dun sistema ou unha rede que está deseñada para bloquear o acceso non autorizado, permitindo ao mesmo tempo comunicacións autorizadas. Os cortalumes poden ser implementados en hardware ou software, ou nunha combinación de ambos. Os cortalumes utilízanse con frecuencia para evitar que os usuarios de Internet non autorizados teñan acceso a redes privadas conectadas a Internet, especialmente intranets.

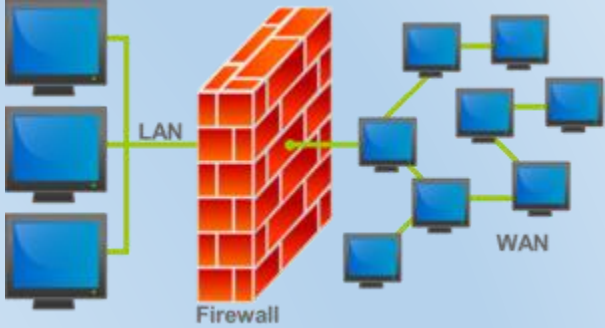
Para explicalo faremos unha similitude entre as portas dunha habitación e os portos dun computador. As conexións ao teu computador fanse a través de portos. Os portos son como portas de acceso ao teu computador; un firewall o que fai é pechar con chave esa porta para que ninguén poida entrar nin saír por aí. As conexións poden ser de entrada ou saída, o que implica que a porta pode utilizarse para entrar ou para saír. É dicir, se un programa do teu computador envía datos a Internet, está a usar a porta para saír, pero se está a recibir datos desde Internet, está a usar a porta para entrar. O cortalumes podería pechar a porta só nun sentido, de forma que só póidase entrar, ou ben só saír. Se usas programas que necesitan comunicarse con Internet, necesitarán que os portos que usan para comunicarse non estean pechados, obviamente.

O cortalumes é moi seguro, pero ten dous problemas:

- É responsabilidade do usuario o decidir que programas se permite que se comuniquen e cales non: pequeno mantemento e esforzo pola túa banda. E ademais podes errar nalgunha desas decisións.
- Ao permitirlle a un programa usar un porto, recae sobre este programa a responsabilidade de evitar calquera ataque de seguridade a través del. Por exemplo, todos temos un navegador instalado, e debemos darlle permiso para comunicarse con Internet. Pero podería darse o caso de que un hacker atopase algún buraco de seguridade no navegador, e lograse coarse no noso PC. Por tanto, dá igual que teñamos instalado o noso firewall se os programas que se conectan a Internet son un auténtico coladeiro.

Os cortalumes tamén teñen limitacións. Teñen que estar bem configurados, pero só poden protexerte de todo o que pase a través deles, e o usuário non debe ser neglixente.

# CORTALUMES (II)




Hai dúas políticas básicas na configuración dun cortalumes:

- Política restritiva: Denégase todo o tráfico excepto o que está explicitamente permitido. Esta aproximación é a que adoitan utilizar as empresas e organismos gobernamentais.
- Política permisiva: Permítese todo o tráfico excepto o que estea explicitamente denegado. Esta aproximación soen utilizala universidades, centros de investigación e servizos públicos de acceso a Internet.

A política restritiva é a máis segura, xa que é máis difícil permitir por erro tráfico potencialmente perigoso, mentres que na política permisiva é posible que non se contemplara algún caso de tráfico perigoso e sexa permitido por omisión.

Os cortalumes por hardware son uns dispositivos que se engaden á rede local e sitúanse entre o punto de acceso a Internet e o "switch" que distribuirá o tráfico da rede ao resto de equipos conectados. O cortalumes por software é unha aplicación que se instala no computador e que se realiza a mesma tarefa que o cortalumes por hardware. A principal diferenza entre ambos os sistemas é o ámbito de traballo de cada un deles. O de software actúa sobre o tráfico de rede que se xera só cara a ou desde o computador no que está instalado. En cambio, no de hardware, é capaz de analizar e filtrar o tráfico de datos que entra ou sae de toda unha rede local, sen importar o número de computadores que estean conectados a ela. Como norma xeral, os cortalumes por hardware utilízanse no ámbito empresarial ou de grandes redes, xa que requiren uns certos coñecementos técnicos e deben ser configurados por administradores de redes. Os de software están orientados a usuarios finais e podes instalalos no teu equipo para mellorar a súa seguridade, pero só protexerá a ese computador. O uso de ambos os sistemas de seguridade informática non é excluínte, como si pode suceder ao instalar dous antivirus nun mesmo equipo.

Para que necesito un cortalumes se xa teño antivirus? Moitos usuarios fanse esa mesma pregunta. A analoxía do porteiro de discoteca talvez poida ser útil para explicar a diferenza entre ambos os sistemas de protección. Diríamos que o cortalumes é o porteiro da discoteca que vixía os accesos e é o encargado de analizar e filtrar aos clientes que entran e saen e de manter as portas abertas ou pechadas. Obviamente, este porteiro non pode saber que está a suceder no interior do local. De vixiar que todo no interior da sala transcorra con total seguridade, tanto para os clientes que xa están dentro, como para o propio negocio, encárgase o persoal de seguridade da sala, que neste caso é o software antivirus.


# Protocolos HTTP e HTTPs

Existen dous "tipos de páxinas" (dous protocolos diferentes) que visualmente diferéncianse por empezar con http: ou por https: (notar o *"s"* do último caso) e por un cadeado pechado ou unha chave que aparece na parte inferior do navegador. A diferenza estriba en que no primeiro caso toda a transmisión faise en claro e a segunda faise cifrada e oculta co protocolo de seguridade SSL (Secure Sockets Layer).

No primeiro caso, os datos transmitidos poderían ser interceptados e, ao ir visibles, poderían apoderarse da información transmitida. A segunda utilízana os servidores para facer transaccións seguras (por exemplo ventas, operacións bancarias, etc) xa que a información é transmitida cifrada. Dentro da categoría de servidores seguros tamén os hai uns máis seguros que outros dependendo do nivel de cifrado.

Unha proba rápida para comprobar a veracidade da web é dar un "dobre click" sobre o cadeado amarelo que aparece na parte inferior/dereita do noso navegador para que saia o certificado de autenticidade da web.

# Clave perfecta en Internet

Imos dar unhas pequenas normas para ter unha clave máis segura dos seus datos:

A) Non usar NUNCA claves que sexan só palabras, por exemplo nomes comúns, nin do usuario, personaxes famosos (políticos, deportistas, etc), membros da familia ou entorno incluídas as mascotas, cousas moi comúns en usar, marcas, cidades, lugares turísticos ou vacacións.

B) Non usar NUNCA claves completamente numéricas que poidan ou non relacionarlle con vostede. Os exemplos máis comúns que usa equivocadamente a xente con claves numéricas son os números de teléfono, datas de nacemento, D.N.I. - C.I.F , números de seguridade social, matrícula do seu automóbil,...

C) Modelo de clave perfecta é que conteña e mesture caracteres alfanuméricos, tamén podemos escoller caracteres do noso teclado, elixidos ao chou. Un pequeno exemplo: Zx89ñ$.qe2

D) Cantos máis caracteres teña, mellor, pero nunca menos de 8 caracteres.

E) Non compartir as súas claves é fundamental.

F) Non usar a mesma clave para todo é mellor, claves distintas para cada un dos seus correos, máquinas ou contas de bancos, pense que se unha persoa obtén dalgunha forma ilícita a súa clave podería ser usada facilmente en todo o que ten e toda a súa seguridade quedaría rota facilmente.

G) Cambiar as claves tras un período de tempo, por exemplo cada 3 meses. Nalgúns bancos forzan aos seus clientes a realizalo para ter unha mellor seguridade para os seus clientes.

Todas estas normas son para ter un pouco máis seguro os nosos pequenos datos persoais ou de empresa desas persoas que poidan usar os nosos datos ilegalmente. É bo pór boas fechaduras á nosa casa para que non poida ser tan facilmente atacadas por intrusos.

# Sistemas de vixilancia electrónica mundiais

ECHELON é considerada a maior rede de espionaxe e análise para interceptar comunicacións electrónicas da historia. Controlada pola comunidade UKUSA (Estados Unidos, Reino Unido, Canadá, Australia e Nova Zelandia), ECHELON pode capturar comunicacións por radio e satélite, chamadas de teléfono, faxes e correos electrónicos en case todo o mundo e inclúe análise automática e clasificación das interceptacións. Estímase que ECHELON intercepta máis de tres mil millóns de comunicacións cada día.

Esta intercepción sería un enlace de antenas, radares e satélites, recibindo apoio de submarinos e avións espía, todos unidos a través de bases terrestres, e o seu obxectivo é espiar as comunicacións mundiais, segundo din para loitar contra o terrorismo internacional e o tráfico de drogas. Segundo algunhas fontes, a rede Echelon dispón de cento vinte estacións e satélites xeoestacionarios.

A pesar de ser desenvolvida co fin de controlar as comunicacións militares da Unión Soviética e os seus aliados, sospéitase que na actualidade ECHELON é utilizada tamén para atopar pistas sobre tramas terroristas, plans do narcotráfico e intelixencia política e diplomática. Os seus críticos afirman que o sistema é utilizado tamén para a espionaxe económica de calquera nación e a invasión de privacidade en gran escala. A existencia de ECHELON foi feita pública en 1976 por Winslow Peck.

# Rede Echelon

Os membros desta alianza levan reunindo intelixencia desde a Segunda Guerra Mundial. O sistema está baixo a administración da NSA (National Security Agency). Esta organización conta con 100.000 empregados tan só en Maryland (Estados Unidos) (outras fontes falan de 380.000 empregados a escala mundial), polo que é probablemente a maior organización de espionaxe do mundo. A información é enviada desde Menwith Hill (Reino Unido) por satélite a Fort Meade en Maryland (EEUU).

A cada estado dentro da alianza UKUSA élle asignada unha responsabilidade sobre o control de distintas áreas do planeta:

- A tarefa principal de Canadá adoitaba ser o control da área meridional da antiga Unión Soviética. Despois da guerra fría púxose maior énfase no control de comunicacións por satélite e radio en Centro e Sudamérica, principalmente como medida para localizar tráfico de drogas e secuaces na rexión.
- Os Estados Unidos, coa súa gran cadea de satélites espías e portos de escoita controlan gran parte de Latinoamérica, Asia, Rusia asiática e o norte de China.
- Gran Bretaña intercepta comunicacións en Europa, Rusia e África.
- Australia examina as comunicacións de Indochina, Indonesia e o sur de China,
- Nova Zelandia vixila o Pacífico occidental.

A rede de espionaxe fóra do control xudicial supón unha privación da liberdade individual consagrada en diferentes textos lexislativos internacionais e nacionais; sendo este o motivo polo que o 21 de outubro de 2001, organizouse a través de Internet un intento de colapsar ou socavar a Echelon.

# Outros sistemas de vixilancia

PRISM é un programa do Goberno estadounidense, que pode ser considerado como parte da rede ECHELON. É divulgada a súa existencia polos medios de comunicación en xuño de 2013, e caracterízase por capturar os datos de compañías como Google, Apple, Microsoft ou Facebook. Aínda que todas elas negan a súa participación activa, a filtración dunha presentación da NSA fai considerar que isto non é así.

Unha rede similar é a Enfopol, da Unión Europea, aprobada polo Consello Europeo en maio de 1999. O seu campo de acción suponse limitado á Unión. Atribúense tamén redes parecidas a Francia (coñecida como Frenchelon) e Rusia (que se chamaría Sorm), debido ás súas situacións xeográficas e ao control e capacidade de actuación que posúen sobre as súas "antigas colonias". Suíza ten a súa propia rede, chamada Satos3 (agora Onyx).

O software de espionaxe Carnivore é unha ferramenta empregada pola axencia federal de intelixencia de Estados Unidos, que usan para rastrexar e analizar as comunicacións en Internet de persoas que se atopan baixo a súa vixilancia. Esta ferramenta instálase nos provedores de acceso a Internet cun permiso xudicial, pode rastrexar todo o que faga un usuario ao conectarse en Internet.