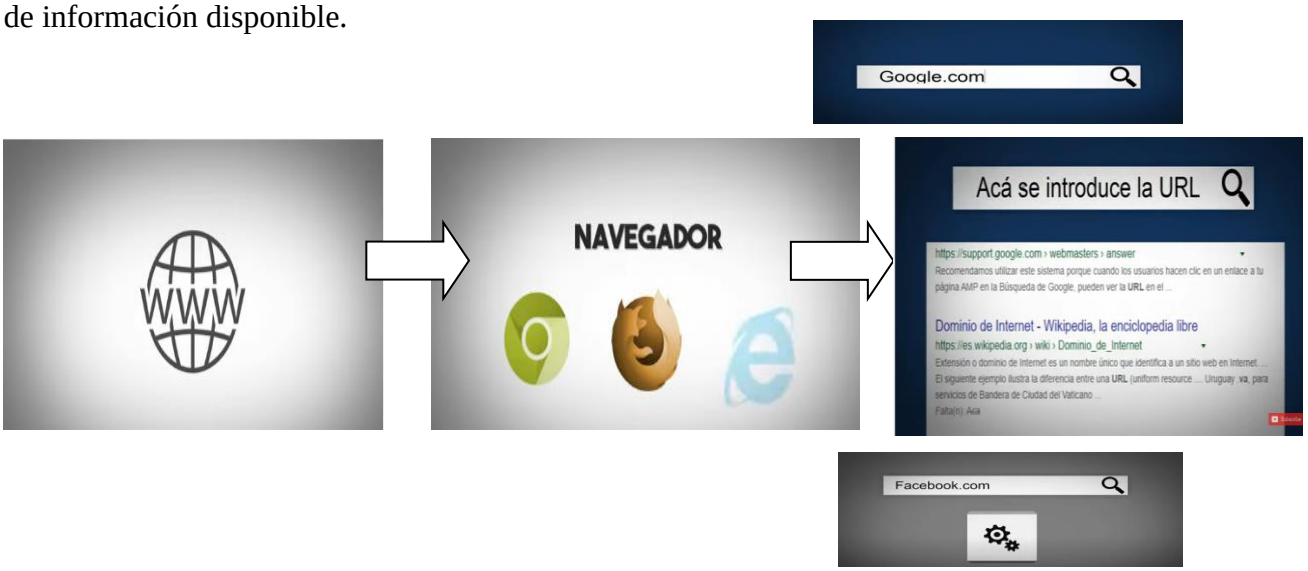
SEGURIDAD en la RED

Todo el mundo debe ser conciente de las amenazas de la red y tenemos que saber como cuidarnos y cuidar la información que le estamos permitiendo que el atacante pueda conseguir. Para poder proteger nuestra información y evitar que nos roben los datos que podrían vulnerar nuestra privacidad o dañar nuestros equipos, es necesario saber cómo funciona la Web.

La World-Wide-Web o w.w.w. como la conocemos más comúnmente, es en español “Red informática mundial”, la que nos permite compartir documentos, que contienen hipertextos o hipermedia y que están conectados a través de internet donde se puede encontrar un montón de información disponible.



A ella accedemos a través de un navegador, o motor de búsqueda, al que le proporcionamos una dirección U.R.L. para que busque información sobre un tema; el mismo nos devuelve una página web que puede contener un texto, sonido, imagen, videos, enlaces y muchas otras cosas más. La web es la mayoría de las veces el medio por las que un ordenador o dispositivo móvil accede a los virus y es también el medio que utilizan los hackers para robarnos información con el fin de obtener algún beneficio.

Esas devoluciones adaptadas al formato que conocemos como de páginas web, se estructuran con un lenguaje de etiqueta como por ejemplo HTML, además suelen contener CSS, lenguaje con los que se personaliza una WEB y a veces también JS Java Script que es el Lenguaje de programación para el front- end o para hacer interactuar los elementos de la

pagina con el cliente y también algún lenguajes de Back- end o el que corra en el servidor que almacenan datos en una base de datos y demás tareas que un lenguaje como JS no podría realizar.

PERO EL PROBLEMA ES ¿CÓMO NOS PROTEGEMOS?

Las maneras de protegernos en la Web son diversas. Usar un buen antivirus, un VPN (proveedor personal de servicios seguros), usar un navegador anónimo y otras cosas suelen proteger. En algunos casos protegemos información, en otros se crea una especie de protección defensiva como una especie de escudo o sea que no nos protegemos atacando sino nos protegemos evitando que algo nos ataque aunque esto no es suficiente.
En resumen o utilizamos algo para que el atacante no obtenga información que le podemos llegar a brindar en el ordenador, o en el otro caso nos defendemos para que el atacante no pase el límite del navegador y se instale de manera remota en nuestros aparatos y dispositivos.

- ✓ ANTIVIRUS
- ✓ NAVEGADOR ANÓNIMO
- ✓ VPN (Seguro)

LAS REDES SOCIALES.

Otro consejo importante es cuidar lo que hacemos en redes sociales, lo que publicamos parece muy básico pero no lo es y no hablo solo de publicar documentos, facturas, datos, que son cosas privadas y demás sino que hablo de otras cosas. Un atacante puede acceder a datos que son reveladores, a datos personales e invadir nuestra privacidad con las cosas que publicamos, también pueden conocer la ubicación de alguien es algo muy sencillo a través de lo que publicamos en nuestras redes sociales.

CUIDADO CON LOS QUE DESCARGAMOS.

Ahora también hay que tener cuidado con lo que descargamos, por que las descargas son una fuente gigantesca de virus y estos pueden entrar a nuestro ordenador de manera muy sencilla, basta con abrir eso que descargamos para que no nos corra un Script que nos puede dañar el ordenador o hacer cosas aún peores.

Todos sabemos que al realizar descargas podemos dañar nuestras computadoras. Tenemos tres tipos de software que podrían llegar a ser dañinos para nuestro ordenador o cualquier tipo de dispositivos con el que accedamos a realizar la descarga.

Software Malicioso que es cualquier software o aplicación móvil diseñado especialmente para hacer daño a algún equipo o bien para dañar software y/o instalar software sin consentimiento del usuario, o también virus, que a veces, los Webmasters no se dan cuenta de que sus archivos se consideran software malicioso y pueden que alojen tales binarios sin saberlo.

El software no deseado es otro tipo de software que provoca comportamientos engañosos inesperados o que perjudican al usuario cuando utiliza el equipo o navega, por ejemplo software que provoca cambios en la página principal u otras opciones de configuraciones del navegador sin que los solicite o aplicaciones que filtraran información privada personal sin informar de ello.

Por último también tenemos Software sospechoso que básicamente tiene las características de que por ejemplo la dan a entender al navegador que probablemente sea inseguro.

Ahora bien conociendo los tipos de descargas con malware que podamos llegar a realizar a partir de ahora es mejor realizar lo siguiente:

Primero asegurarnos de que se trata de un sitio web de confianza, después tenemos que verificar que el candadito de seguro este. Si es un archivo que tenemos que descargar, si o si, pero no estamos seguros de que realmente sea el archivo que buscamos es recomendable descargarlo desde una máquina virtual, verificar la fuente, links similares etc. Primero para verificar su veracidad, para luego finamente descargarlo en nuestros ordenadores o dispositivos móviles y por último no descargar esos archivos en un ciber, para validar que sea seguro, porque podríamos perjudicar a personas que están prestando un servicio.

LAS CONTRASEÑAS.

Pasamos a una de las cosas más importantes, que todo el mundo tiene que tener en cuenta, trabajar en esto es muy importante, hablaremos ahora de las contraseñas.

Cuando nosotros ponemos una contraseña, estamos tratando de que esa contraseña sea indescifrable, para un humano y que no pueda acceder a nuestra clave o por lo menos entrar a nuestra cuenta sin forzarla. Pero ¿ustedes creen que los humanos van a probar clave por clave? Los que intentan descifrar las contraseñas, no son los humanos, sino sistemas que están programados para eso, por ende una contraseña corta no nos va a funcionar, lo que más nos va a funcionar es una contraseña larga.

Hay ciertos parámetros que se deben tener en cuenta, por ejemplo en el caso de los Password Biométricos (huellas), las cadenas con Token o simples cadenas. Pero ¿qué debe tener un password para ser bien seguro?

Primero que una persona no pueda adivinarla, después que los sistemas automáticos tampoco puedan adivinarla y por último que la recordemos aunque esto no necesariamente implica seguridad pero al fin y al cabo es algo muy relevante.

Veamos los tres casos más comunes para utilizar una contraseña, primero para las redes sociales, disponibles para la red WiFi y después para desbloquear celulares o dispositivos. Empecemos por el primero tanto para las Redes Sociales como para Wi Fi debemos utilizar un mínimo de 8 caracteres a pesar de que algunos permiten más, ¿qué se debe hacer para hacerlos bien seguros? no debemos crear una contraseña como respuesta a preguntas personales, por ejemplo el nombre de tu mascota, la fecha de nacimiento o la de un familiar, nombres personales públicos etc.

El programa que descifra contraseñas son extensos y hacen una especie de prueba donde arrancan de pocos caracteres hasta finalizar con muchos y a pesar de que agregamos números, tampoco lo haremos más seguro de hecho les tomara menos de un segundo a el programa, descifrar esos nuevos números.

Para tener una contraseña bien segura deberíamos hacerla largo ya que esto hace que tanto las personas como las maquinas requerirán más tiempo para descifrarla; también deberíamos utilizar caracteres especiales mayúsculas y minúsculas y de uno a cuatro números, de esta forma acceder a ella podrá ser cada vez más complicado o sea que las probabilidades de que se pueda descifrar tu clave son más reducidas.

Ahora para la contraseña de celulares, tablets y demás donde utilizamos PIN o algún otro método solo deberíamos hacerlo lo más larga que se pueda y no utilizar simbolismos que claramente estén vinculados a su vida pública o emocional por ejemplo las letras de su nombre, cuadrados y demás.

EL HACKING

Ahora nos vamos a meter de lleno en el terreno del Hacking pero lo primero será definirlo. Hay un concepto muy erróneo que la gente toma en cuenta por la televisión y los medios y está mal. Un hacker no es esa persona malvada que te roba las contraseñas que se mete en tus sistemas y demás. Un hacker es una persona que se encarga de hallar debilidades en un sistema para poder mejorarlo y hacerlo más seguro, de hecho eso es la función principal de un hacker. Tenemos los Black hat hackers y los White hat hackers, unos son los buenos y otros son los malos. Los hackers no necesariamente son malos lo importante no está en la herramienta sino en para que se utiliza.

ALGUNAS DE LAS TÉCNICAS MÁS USADAS EN LA ACTUALIDAD PARA SEGUIR A LAS PERSONAS,
PARA QUE SIRVEN O COMO FUNCIONAN

Las técnicas más conocidas y más importantes, que afectan a los usuarios individuales no a las empresas; usan estas técnicas, lo hacen con la finalidad de obtener datos o algo que les genere una rentabilidad o un beneficio propio o simplemente para espiar.

- ✓ CLICKJACKING
- ✓ PHISHING
- ✓ EAVESDROPPING
- ✓ FAKE WAR
- ✓ KEYLOGGER

Todos creemos que los atacantes quieren hackear a las empresas para poder robar dinero, pero en realidad según la mayoría de los manuales de ciberamenazas, casi la mitad de los atacantes en la Web buscan el robo de datos sensibles, el 25% aproximadamente tiene como objetivo influir en procesos políticos y sociales, mientras que el 20% rastrea la red en busca de dinero y el otro 5% provienen del terrorismo. Pero en estas maneras de hackear existen realmente miles de posibilidades distintas.

- ✓ *https://www.thalesgroup.com/es/group/journalist/press-release/cyberthreat-handbook-thales-verint-lanzan-su-quien-es-quien-los*
- ✓ *https://www.verint.com/engagement/our-offerings/solutions/security/*

Vamos a centrarnos en cinco técnicas más usadas en la actualidad:

CLICKJACKING consiste en que el atacante usa varias capas transparentes u opacas para engañar al usuario y así poder ocultar algo. El usuario engañado hace click en su botón y esto lo lleva a otro enlace en otra página, cuando en realidad intentaba hacer click en la página de nivel superior.

Por ejemplo imaginen que un atacante crea un sitio web que tiene un botón que te dice clickea aquí para ganar un Iphone, pero en esa página web el atacante cargo un iframe (anidado, que

Permite incrustar otra página HTML en la página actual), que básicamente agarra una parte de una página y lo pone en la nuestra y este iframe es un informe con su cuenta de correo, información confidencial o puede incluso tomar control de nuestro ordenador. En uno de los muchos navegadores web o plataformas con alguna vulnerabilidad, un ataque de clickjacking puede tomar la forma de código embebido o script que se ejecuta sin el conocimiento del usuario. Por ejemplo: aparentando ser un botón para realizar otra función.

PHISING

Es una técnica para obtener información personal privada sobre otro, como su nombre de usuario, contraseña y detalles de tarjetas de crédito, fingiendo la identidad de otra persona, o entidad de confianza, mediante un mensaje de correo electrónico o a través de una página Web. Por ejemplo nos envían un mail de Instagram, solicitándole que inicie sesión en su cuenta, para verificar su identidad; además nos dicen que, en caso de que no lo haga su cuenta estará cancelada. Uno persona entra y envía sus datos y se muestra un mensaje de que puso los datos en forma incorrecta, así que los rellena de nuevo, y esta vez si logra entrar. Pero lo que acaba de pasar es que sin darse cuenta el correo donde acaba de mandar sus datos no provenía de Instagram sino de otro lado ; provenía del servidor del atacante que cuando entro al enlace y envió nuevamente sus datos, en realidad no puso los datos incorrectos sino que lo que sucedió allí es que los datos no se estaban siendo enviados a Instagram sino que se

estaban registrando en una base de datos del atacante, por ende el atacante mostró que sus datos eran incorrectos en la página oficial de Instagram y acabo por darle sus datos a los atacantes.

EAVESDROPPING este método consiste en un ataque pasivo en el cual los sistemas informáticos y las redes se supervisan para que un pirata informático obtenga cierta información. Un sniffer de internet (analizador de protocolos) es un programa que trabaja en forma conjunta con la tarjeta interfaz de red para absorber indiscriminadamente todo el tráfico que este dentro del umbral de audición del sistema de escucha y recibirá todos los paquetes que se desplazan por la red. El objetivo de ese método no es causar daños a la computadora sino recolectar información a medida que se transmite.

FAKE WAP Todos visitamos lugares donde hay WI FI gratis algunos restaurantes, locales u otros sitios donde se puede acceder fácilmente a internet, pero algunos atacantes pueden utilizar software y tarjetas inalámbricas para configurar una IP falsa en un lugar público, simulando una red real. Entonces cuando nos conectamos a su red ellos automáticamente tienen el control sobre toda la información que enviamos, documentos, contraseñas, y así las cosas privadas son capturadas por los atacantes. La información se envuelve en paquetes, o sea lo desempaquetan a través de la red que tiene la capacidad de hacerlo y obtiene así la información enviada, como contraseñas, usuarios, etc.

Para que puedan usar su red se creen una cuenta; esos datos pasan a la Base de Datos del atacante, pero lo que ocurre es que las personas utilizan las mismas claves, dos o tres contraseñas para todo entonces cuando realizan el registro las probabilidades de que sus datos coincidan con los de otro sitio web popular son altas así pueden acceder a su cuenta de Facebook, Instagram, twitter, sitios de cuentas bancarias entre otros ya que las contraseñas probablemente coincidan.

KEYLOGGER Es un software o un hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya previamente infectado con este malware. Este malware se sitúa entre el teclado y el sistema para interceptar y registrar la información sin que el usuario lo note. Además un Keylogger almacena datos en forma local en el ordenador infectado y permite que el atacante tenga acceso remoto al equipo de la víctima y registrar información del otro equipo. De esta forma podemos escribir contraseñas, mails entre otros y todo este podría ser almacenado por el atacante.

¿Cómo protegernos de cada una de estas técnicas?

- ✓ Ya sabemos cómo funcionan estas técnicas ahora veremos cómo protegernos de cada una de estas técnicas. No hay un único antivirus que proteja de todo ni hay una única protección que sirva para todo por ende para cada ataque debemos protegernos de una manera distinta.

- ✓ La protección depende más del usuario que del sistema, ya que hay que conocer un poco de seguridad para poder evitar instalar una herramienta de seguridad, para aplicaciones web como *NO SCRIPT O NOT SCRIPT* para identificar sitios no confiables y para que nuestro navegador reconozca los sitios de los que no confiamos.
- ✓ El usuario debe ser muy precavido para poder evitar ataques, ya que estos adoptan la forma de empresas reales y llevan como remitente el nombre de la empresa o el nombre del empleado de la empresa, además incluyen webs visualmente iguales a las empresas reales, como gancho utilizan regalos, o la amenaza de la pérdida de la propia cuenta. En caso de que se desconozca la procedencia del mail, es aconsejable preguntar llamando a la empresa o a la persona que envió el mail y consultar si esa es su dirección
- ✓ Usar un VPN, evitar el tráfico HTTP y en la redirección a sitios HTTP verificar que siempre sea HTTPS ya que la "S" significa secure e indica que tiene un cifrado seguro.
- ✓ Si existen dos redes y una dice gratis existen muchísimas posibilidades que sea un ataque porque generalmente al decir "gratis" las personas entran. Ante esto preguntar al dueño de las dos redes cual es la correcta.
- ✓ En una red pública jamás realizar una transacción financiera ni acceder a sus cuentas bancarias u otras cuentas que tengan con información financiera independientemente si la red es confiable o no.
- ✓ Actualizar el Software antivirus de los teléfonos a la última versión para estar más seguros que tendrán más eficiencia a la hora de protegernos.
- ✓ No instalar ningún software gratuito que este pirateado o parezca sospechoso.
- ✓ Cambiar las claves cada cierto tiempo, por ejemplo una vez al mes, para navegar por la web y/o jugar.
- ✓ Usar un perfil de privilegios limitados en tu sistema operativo. Usar un navegador moderno y actualizado como el Chrome y por ultimo realizar backup de datos o sea una copia para evitar perdida de datos de tu cuenta.