Instituto Nacional
de Tecnologías
de la Comunicación

Política de contraseñas y seguridad de la información

En los últimos años, el perfil de los usuarios de Internet y los usos que estos hacen de la Red, ha variado, alcanzándose unas notables tasas de penetración en determinados servicios. Así, por ejemplo en España, el correo electrónico, con un 99,5%, es el servicio más utilizado entre los usuarios habituales de Internet entre 16 y 74 años, un 63% ha utilizado servicios de banca electrónica y actividades financieras y el 52% ha realizado compras online.[1]

El resultado de todo este proceso de incorporación a la sociedad de la información es que el número de dispositivos desde los que se puede acceder a las redes de información se ha ampliado, y las gestiones desde los mismos son más numerosas, más frecuentes, y de mayor trascendencia económica.

En este contexto, y con el objetivo de que todo el proceso de comunicación sea gestionado de forma segura, a la hora de hacer dichos usos y transacciones a través de Internet, han de tomarse una serie de medidas y buenas prácticas encaminadas a mejorar la seguridad. En este sentido, la concienciación del usuario para gestionar de modo eficiente su información tiene uno de sus pilares en la correcta gestión y creación de las contraseñas que este ha de utilizar en la mayoría de los procesos y operaciones que requieren de su autenticación.

Habitualmente, cuando un usuario pretende realizar una transacción con una empresa por medio de la Red le es requerida una clave de usuario (*login*) y una contraseña (*password*). Así, en el 24% de los casos de las empresas que ofrecen sus servicios a través de Internet, el usuario ha de registrarse como tal e identificarse para acceder a dichos servicios mediante una contraseña.[2]

Sin embargo, observando los datos estadísticos sobre usos y hábitos en Internet, se constatan carencias y lagunas en la gestión de la seguridad de la información en relación con el empleo de las contraseñas. En general, sólo el 41% de los usuarios habituales de Internet españoles utiliza claves o contraseñas como medidas de seguridad[3] y, en

[1] INTECO: Estudio sobre la Seguridad de la Información y e-Confianza de los hogares españoles (1ª Oleada:Dic-Ene 07)-www.inteco.es

[2] INE: Encuesta sobre el uso de TIC y comercio electrónico en las empresas (2005-2006). www.ine.es

[3] Red.es: XI oleada del panel de “las TIC en los hogares españoles”. www.red.es

particular, apenas la mitad (51,6%) utiliza dicha medida para el acceso y protección de los ficheros ubicados en los ordenadores domésticos.[4]

Sin embargo, y a pesar de ser una medida de seguridad no demasiado extendida, la importancia de la utilización y robustez de las contraseñas y claves es muy elevada.

Debemos ser cuidadosos a la hora de elegir nuestras contraseñas

Tanto en el ordenador del trabajo, como en el propio del hogar existe información y se realizan operaciones cuya repercusión económica y personal es muy importante. Esto afecta al los sistemas de las empresas y equipos informáticos, así como a la privacidad del usuario. A ninguno se nos ocurriría dejarle la llave de nuestro hogar a cualquier desconocido que nos la pidiera, incluso al perderla se procede a cambiarla inmediatamente. Algo parecido sucede con nuestras contraseñas.

A nadie se le ocurriría dejarle el nombre de usuario y contraseña de acceso a nuestros servicios bancarios por la Red a un desconocido, o siquiera, a un conocido. La repercusión de este hecho puede suponer desde que nos *vacíen* la cuenta suplantando nuestra persona, o en el caso de nuestro trabajo, que se apoderen de todos los datos en nuestro equipo contenidos o, incluso, puedan eliminarlos, perdiendo hasta años de trabajo por una descuidada gestión de nuestras contraseñas. Un reciente estudio elaborado entre 325 empleados señala que un 30% de trabajadores americanos guarda sus contraseñas, apuntadas en un papel cerca del propio equipo, y un 66% lo hace en un archivo en su propio ordenador o en su móvil. Estas conductas poco cuidadosas facilitan enormemente las incidencias de seguridad que, de ocurrir, pueden llegar a tener consecuencias graves.

Así, el "*phishing*", uno de los fraudes más extendidos últimamente por la Red, precisamente centra su objetivo en conseguir las claves y contraseñas del usuario, para usarlas con fines espurios. Así, en el caso más habitual se suplanta la página web de una entidad bancaria o financiera (aunque pueden ser también páginas de la administración, buscadores, subastas) para de este modo, robar los datos del usuario y realizar operaciones y transacciones económicas en su cuenta bancaria.[5]

[4] INTECO: Estudio sobre la Seguridad de la Información y e-Confianza de los hogares españoles (1ª Oleada:Dic-Ene 07)-www.inteco.es
[5] INTECO: Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing. www.inteco.es

Consecuencias de la sustracción o revelación de nuestras contraseñas

El objetivo de la sustracción de nuestras contraseñas para con ellas apropiarse de información sensible para el usuario con una finalidad de tipo económico o bien realizar otras acciones dañinas o delictivas como borrado de toda información, chantaje, espionaje industrial, etc. Las consecuencias son diversas y varían según el valor que cada usuario haya establecido para la información.

Por ejemplo, si la contraseña corresponde a la de un servicio bancario podrían sustraernos dinero de la cuenta o efectuar otras operaciones con perjuicio económico para el usuario.

Si la contraseña pertenece al ordenador de nuestro hogar podrían tomar su control o robar toda la información contenida en él: como otras contraseñas o listados de usuarios y correos electrónicos o archivos personales y documentos. Otra consecuencia podría ser el borrado completo de toda la información allí incluida.

En el ámbito laboral, las consecuencias pueden llegar a ser catastróficas si un tercero suplanta nuestra identidad utilizando nuestro usuario y contraseña. Así, podría acceder a los sistemas corporativos con nuestro usuario y, bien sustraer todo tipo de información del trabajador y/o la empresa, o bien utilizar esta entrada para modificar o incluso eliminar archivos, con las consecuencias económicas, de responsabilidad jurídica y pérdidas de imagen que ello supondría.

Métodos por los que nuestras contraseñas quedan al descubierto

Los métodos para descubrir las contraseñas de un usuario son variados. En primer lugar, se basan en la utilización de la "*ingeniería social*", por ejemplo utilizando el teléfono o un correo electrónico para engañar al usuario para que éste revele sus contraseñas. Dentro de este grupo destaca el fraude conocido como "*phishing*". En este tipo de estafa online el objetivo consiste en obtener las contraseñas o número de la tarjeta de un usuario, mediante un e-mail, sms, fax, etc. que suplanta la personalidad de una entidad de confianza y donde se le insta al usuario que introduzca sus contraseñas de acceso.

También es posible que el usuario se la comunique o ceda a un tercero y, por accidente o descuido, quede expuesta al delincuente, por ejemplo, al teclearla delante de otras personas. Puede ser que el atacante conozca los hábitos del usuario y deduzca el sistema que éste tiene para crear contraseñas (por ejemplo, que elige personajes de su libro favorito) o que asigne la misma contraseña a varios servicios (correo electrónico, código PIN de las tarjetas de crédito o teléfono móvil, contraseña de usuario en su ordenador, etc.).

Otro método, consiste en que el atacante pruebe contraseñas sucesivas hasta encontrar la que abre el sistema, lo que comúnmente se conoce por "*ataque de fuerza bruta*". Hoy en día un atacante, con un equipo informático medio de los que hay en el mercado, podría probar hasta 10.000.000 de contraseñas por segundo. Esto significa que una contraseña creada con sólo letras minúsculas del alfabeto y con una longitud de 6 caracteres, tardaría en ser descubierta, aproximadamente, unos 30 segundos. Igualmente, se aplican técnicas más sofisticadas para realizar la intrusión. Se trata de métodos avanzados que en consiguen averiguar la contraseña cifrada atacándola con un programa informático ("*crackeador*") que la descodifica y deja al descubierto.

Un último grupo de técnicas se basan en la previa infección del equipo mediante código malicioso: con programas "*sniffer*" o "*keylogger*". Un programa "*sniffer*" o "*monitor de red*" espía las comunicaciones del ordenador que tiene residente dicho *malware*, a través de la red, y de ellas obtiene los datos de las claves. El "*keylogger*" o "*capturador de pulsaciones de teclado*" consiste en un programa que se instala en el ordenador del usuario de modo fraudulento, y almacena en un archivo toda aquella información que se teclea en el ordenador. Más adelante dicho archivo puede ser enviado al atacante sin conocimiento ni consentimiento del usuario y, con ello, el intruso puede obtener las distintas contraseñas que el usuario ha utilizado en el acceso a los servicios online o que ha podido incluir en correos electrónicos .

Recomendaciones de INTECO en relación a la gestión y establecimiento de contraseñas.

Para gestionar correctamente la seguridad de las contraseñas, desde el Instituto Nacional de Tecnologías de la Comunicación (INTECO) se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

Política y acciones para construir contraseñas seguras:

1. Se deben utilizar al menos 8 caracteres para crear la clave. Según un estudio de la Universidad de Wichita, el número medio de caracteres por contraseña para usuarios entre 18 y 58 años habituales de Internet es de 7. Esto conlleva el peligro de que el tiempo para descubrir la clave se vea reducido a minutos o incluso segundos. Sólo un 36% de los encuestados indicaron que utilizaban un número de caracteres de 7 o superior.

2. Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.

3. Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula. Según el mismo estudio, el 86% de los usuarios utilizan sólo letras

minúsculas, con el peligro de que la contraseña sea descubierta por un atacante casi instantáneamente.

4. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.

5. Las contraseñas hay que cambiarlas con una cierta regularidad. Un 53% de los usuarios no cambian nunca la contraseña salvo que el sistema le obligue a ello cada cierto tiempo. Y, a la vez, hay que procurar no generar reglas secuenciales de cambio. Por ejemplo, crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña. P. ej.: pasar de “01Juitnx” a “02Juitnx”.

6. Utilizar signos de puntuación si el sistema lo permite. P. ej.: “Tr-.3Fre”. En este caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, hay que comprobar primero si el sistema permite dicha elección y cuáles son los permitidos. Dentro de ese consejo se incluiría utilizar símbolos como: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

7. Existen algunos trucos para plantear una contraseña que no sea débil y se pueda recordar más fácilmente. Por ejemplo se pueden elegir palabras sin sentido pero que sean pronunciables, etc. Nos podemos ayudar combinando esta selección con números o letras e introducir alguna letra mayúscula. Otro método sencillo de creación de contraseñas consiste en elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc. Con ello, mediante esta sencilla mnemotecnia es más sencillo recordarla. Vg: de la frase “Comí mucho chocolate el domingo 3, por la tarde”, resultaría la contraseña: “cmCeD3-:xLt”. En ella, además, se ha introducido alguna mayúscula, se ha cambiado el “por” en una “x” y, si el sistema lo permite, se ha colocado algún signo de puntuación (-).

Acciones que deben evitarse en la gestión de contraseñas seguras:

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas. Un 55% de los usuarios indican que utilizan siempre o casi siempre la misma contraseña para múltiples sistemas, y un 33% utilizan una variación de la misma contraseña.

2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el DNI o número de teléfono.

3. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)

4. No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

5. Hay que evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.

6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.

7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).

8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador),

9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios: Este método de ataque es conocido como *“ataque por diccionario”*.

10. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.

11. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos. En este caso debe existir un sistema de recarga de la contraseña o “*vuelta atrás*”.

12. No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.

13. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).

14. Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

Herramientas y soluciones informáticas

Existe también la posibilidad de recurrir a herramientas y soluciones de software que creen las contraseñas seguras que vamos a utilizar. A continuación, ofrecemos una recopilación de enlaces que pueden ser de utilidad al usuario:

- MaxPassword: http://www.max2k.com/
- lameGen: http://lame-industries.net/
- ViPNet Password Roulette: http://www.infotecs.biz
- Password Generator: http://www.wincatalog.com/
- Password Strength Analyser and Generator: http://pwdstr.sourceforge.net/
- Cryptix: http://www.rbcafe.com/