RESUMEN FINAL DEL CURSO: PUNTOS MÁS RELEVANTES

La veloz evolución de Internet ha cambiado nuestras vidas de forma significativa teniendo acceso inmediato a gran cantidad de información; posibilitando la interacción con amigos, desconocidos y/o empresas; teniendo servicios virtuales a un solo clic y ofreciendo un espacio virtual para actividades de ocio o profesionales.

El uso de la red ha derivado en que estamos expuestos a grandes riesgos que pueden tener un impacto severo en nuestra vida. A lo largo de nuestro día, constantemente compartimos nuestros datos dejando un rastro que conforma lo que se conoce como **identidad digital** y con ella, nuestra **reputación online;** la imagen que los demás tienen sobre nosotros partiendo de la información que encuentran en Internet. Cada vez que interactuamos en la red es recomendable seguir unas reglas básicas de comportamiento para prevenir situaciones de riesgos y dotar de un entorno respetuoso y amigable para todos. Estas reglas se conocen cómo **netiqueta**.

Es difícil ser consciente de todo el rastro que dejamos al utilizar la red, por tanto, la práctica de ***egosurfing*** nos ayudará a conocer qué hay publicado sobre nosotros. Consiste en utilizar buscadores y redes sociales para buscar datos relativos a nosotros mismos. Siendo consciente de nuestra reputación online podremos alinear con nuestros objetivos y con quién realmente somos y, podremos empezar a tomar acciones para limitar la sobreexposición.

Si encontramos que se está vulnerando nuestra privacidad, podremos ejercer una serie de derechos que tenemos los ciudadanos como la oposición o la supresión de los datos personales que están regulados en **Reglamento General de Protección de Datos (RGPD).**

A la hora de utilizar las **redes sociales** tendemos a compartir gran cantidad de información personal y es importante protegerla. En las redes sociales podríamos sufrir la **suplantación de identidad** que consiste en que un ciberdelincuente se hace pasar por nosotros; podrían robarnos la cuenta accediendo a nuestra información privada; podríamos estar expuestos a contactos, concursos, anuncios fraudulentos pudiendo ser estafados; o incluso ser víctimas de prácticas de ciberacoso o sextorsión. Por tanto, a la hora de utilizar las redes sociales debemos configurar las opciones de privacidad y seguridad, publicar lo estrictamente necesario, no compartir nunca información sensible y evitar entrar en discusiones con desconocidos.

En cuanto a la **navegación** por Internet, también debemos seguir buenas prácticas para proteger nuestra privacidad y seguridad. Antes de empezar debemos tener el navegador y el explorador actualizados. Es importante evitar enlaces dudosos y webs sospechosas. Para ello, debemos comprobar que la web comienza por HTTPS y comprobar que dispone de certificado de seguridad (el icono de un candado a la izquierda de la URL). Tener precaución con las redes wifi públicas, comprobar el historial de navegación, *cookies* y ficheros temporales y utilizar el modo incógnito para las tareas confidenciales.

Al navegar limitar el uso de las ***cookies*** es importante. Una *cookie* simplemente es un pequeño fichero de datos que se almacena en el dispositivo al entrar en una página web, que ayuda a personalizar la página web y mejorar la experiencia de usuario, pero también podemos estar

cediendo nuestra información personal a terceros; por tanto, revisa antes de aceptar las *cookies*, y bórralas frecuentemente.

Borrar la huella que ya tenemos generada online no es fácil, pero lo recomendado es empezar con la práctica de egosurfing para detectar cual es esta huella. Una vez hemos detectado la información que se quiere eliminar lo más efectivo es borrar la cuenta, subscripción o registro. Las redes sociales o servicios web suelen tener la opción de borrar la cuenta en el perfil, si no pudiéramos encontrar la forma se puede utilizar la ayuda y soporte de la propia aplicación o servicio.

Existen muchos tipos de **ciberataques**, de los más frecuentes son conocidos como **ataques de ingeniería social**, que son aquellos en los que los ciberdelincuentes usan técnicas para ganarse nuestra confianza y que hagamos algo o le facilitemos algún tipo de información bajo su manipulación y engaño. Se denomina ***phishing*** cuando tratan de enviar algún archivo malicioso adjunto o enlace a páginas web fraudulentas; cuando el engaño es a través de mensajes de texto se denomina ***smishing*** y cuando es mediante una llamada telefónica **vishing**.

A través de engaños de ingeniería social o simplemente a través de buscadores o enlaces podemos terminar accediendo a una plataforma y tienda electrónicas fraudulenta. Para evitarlo, se deben revisar los avisos legales y políticas de privacidad; verificar las conexiones seguras mediante HTTPS y si se disponen de certificados de confianza, precios estables y equiparables al precio real de mercado; no dejarse llevar por ofertas vertiginosas; evitar enlaces que llevan a descargas de *software* o donde los procesos de pago se realizan en otros apartados que no son pasarelas de pago bancarias (tipo PayPal), etc. Si caemos en una tienda fraudulenta podremos ser víctimas de robo de datos personales y perjuicio económico.

Otro de los temas con los que debemos ser precavidos es con el almacenamiento de nuestra información en la nube. Los espacios donde almacenamos documentos que queremos compartir entre varios dispositivos o tenerlos a salvo por si ocurre algún problema con nuestros dispositivos nos permiten realizar copias de seguridad de la información en un servidor de una empresa o servicio que estará siempre disponible para que nosotros dispongamos de esa información cuando lo necesitemos; pero esta facilidad en almacenar, compartir y recuperar la información hace que nuestra información este más accesible desde cualquier sitio con acceso a información y es fundamental tener contraseñas robustas, administrar correctamente los accesos, usar mecanismos de cifrado y tener las actualizaciones aplicadas.

El punto de entrada por excelencia de nuestra información almacenada (tanto en la nube cómo física son los dispositivos móviles). Por tanto, es fundamental aplicar medidas de seguridad y privacidad a los dispositivos como son el bloqueo de pantalla y tarjeta SIM, mecanismos de encuentra mi dispositivo, notificaciones, permisos cedidos a las aplicaciones, ubicaciones, etc. Si nuestro dispositivo es robado, debemos tratar de localizarlo primero, después cambiar contraseñas y tratar de bloquear/borrar información remotamente y, por último, denunciar la pérdida en la comisaría más cercana.

Acabamos de mencionar las contraseñas robustas como método de protección, pero, ¿qué son? ¿cómo los genero? A pesar de que la seguridad total no existe, las contraseñas que se consideran robustas son más difíciles de adivinar y entre las recomendaciones se encuentran no usar la

misma contraseña; introducir combinación de caracteres, números y letras; utilizar mecanismos de doble factor de autentificación y cambiar la contraseña periódicamente.

Las redes Wifi también tienen sus riesgos por lo que se recomienda evitar realizar acciones que pueden comprometernos a través de las redes wifi públicas (compras online, intercambio de información sensible, cambios de contraseñas, gestiones financieras, etc.) y proteger con contraseña nuestra red de wifi doméstica.

Por último, debemos conocer que en nuestro país disponemos de diferentes entidades públicas, agencias y observatorios encargados de acercar el concepto de la ciberseguridad a la ciudadanía, empresas y a profesionales y también disponemos de una serie de canales de denuncia que nos permiten poner en conocimiento actos o conductas que pudieran ser delictivas. Es más, a veces se comenten delitos sin saber que se están cometiendo.