Proyecto IDCAP: Mejorar la Competencia Digital en Personas Adultas

Número de proyecto: 2018-1-PL01-KA204-051003

Identidad Digital

1. Introducción 3
2. Gestión de la identidad digital 4
3. Gestión de la cuenta de Internet 5
4. Cuestiones de seguridad y privacidad 7
5. Huella digital 9
6. Identidad Online 10
7. Resumen 11
Bibliografía: 12

1. Introducción

En términos de identidad digital o basada en Internet, la identidad digital es la información que representa a una persona real u otro agente externo. El agente externo también puede ser una sola máquina, sistema y/o aplicación.

ISO/IEC 24760-1 define la identidad como "un conjunto de atributos relacionados con una entidad". Hoy en día hablamos de la identidad como atributos particulares de una entidad que ha reemplazado el término "agente". En este documento nos referiremos únicamente a la identidad digital como la identidad de una persona física.

Aquí presentaremos los conceptos básicos de gestión de su identidad digital y por qué es importante protegerla. A continuación, veremos con más detalles cómo administrar una cuenta de Internet y cuáles son los pasos clave en el proceso. Más adelante, presentaremos los conceptos básicos de seguridad y privacidad en línea. Finalmente, discutiremos brevemente sobre la huella digital y los problemas de identidad en línea.

2. Gestión de la identidad digital

Gestión de identidad digital se transmite en base a unos principios, los cuales siguen mecanismos más o menos conocidos, que se desarrollaron para la identidad no digital. Aunque parezca complicado, piense en su tarjeta de identificación. Cuando solicita recibir su tarjeta de identificación, la autoridad que la emite valida con otras autoridades sus datos personales, como por ejemplo, la fecha de su nacimiento, número de seguridad social, número de ciudadano (cuando corresponda), una nueva foto de usted, etc.

En el mundo digital, su identidad digital puede ser tan simple como su nombre de usuario y contraseña o puede tener muchos más niveles de complejidad, que están ahí para garantizar que el propietario de esa identidad en particular sea usted y solo usted. Estos niveles pueden incluir una firma electrónica separada, un *token* para la generación "aleatoria" de un código digital particular, confirmación vía SMS o mediante el envío de un código PIN que se envía a un teléfono móvil particular (que se sabe que está registrado para una persona específica), identificación de voz, respuesta a una pregunta particular (como ¿Cuál fue su primer nombre de mascota?), validación de huellas digitales y muchos otros. Todos esos niveles están sirven para garantizar que solo la persona específica, o usuario, esté autorizada para realizar acciones en el mundo digital bajo esa identidad.

Muchas personas encuentran esos niveles difíciles de entender, confusos y frustrantes. Puede que tengan razón, pero, por otro lado, uno debe entender que el mundo digital es una representación directa del mundo físico y a nadie le gustaría que su dinero "digital" fluya de su cuenta bancaria "real". Las instituciones, y especialmente los bancos, colocan varios niveles de seguridad, no para molestar a los usuarios, sino para proteger su identidad y garantizar el derecho de operaciones y transacciones. Paralelamente, se ofrecen más y más servicios a través de su teléfono móvil. Estos cubren un rango tan amplio que enumeraremos aquí solo algunos como ilustración. Piense en ellos como servicios que influyen directamente en su cuenta bancaria "real". Algunos de

esos servicios realizados a través de teléfonos inteligentes (dependiendo de su país de residencia) pueden ser:

- Pago de estacionamiento por mensaje SMS.
- Pago de su factura en el supermercado.
- Pago de las facturas de su casa.
- Transferencia directa de dinero a través de una aplicación autorizada por la entidad bancaria.
- Pago autenticado en 3D de su VISA o Master Card: después de haber enviado el número de tarjeta, la validez y el código de seguridad, este sistema envía un SMS con un código de 6 dígitos para verificar el teléfono móvil con anticipación, lo que agregará una capa más de protección de las transacciones de su tarjeta.
- Tickets para transporte terrestre (tren, autobús…) y billetes de avión.

Con "Apple Pay" y "Google Wallet", su teléfono móvil se convierte en una billetera para cualquier pago que admita pagos magnéticos o NFC (Near Field Contact), este es un método de pago en el que solo hay que acercar la tarjeta, en este caso el móvil, al dispositivo de cobro, por lo que no hace falta introducir la tarjeta en el dispositivo. Incluso le permite recibir pagos de varios sitios, tiendas y usuarios a través de Internet.

Es comprensible por qué es tan importante administrar adecuadamente su identidad digital y por qué es necesario protegerla vigorosamente.

3. Gestión de la cuenta de Internet

Como parte de su identidad digital, la creación de una cuenta en Internet es, en muchos casos, el inevitable primer paso. Por lo general, esto significa tener una cuenta en un servicio de correo electrónico como, por ejemplo, Gmail de Google, correo de Yahoo!, Outlook de Microsoft, etc. Una vez que haya creado dicha cuenta, tiene que definir, al menos, dos datos para su cuenta en internet: su nombre de usuario y su contraseña.

Además, hoy en día, la mayoría de las ofertas requieren que se adjunte un número de teléfono móvil y se verifique en cada cuenta específica. Por lo tanto, su cuenta en internet cuenta con un mínimo de 3 datos: su nombre de usuario, su contraseña y su número de teléfono móvil.

En muchos casos, esta verificación se lleva a cabo sin preguntarle, pero además, para protegerlo aún más, esta verificación no implica solo el número de teléfono, sino también un número que es único para cada teléfono móvil, el número de producción de los teléfonos móviles, llamado IMEI (International Mobile Equipment Identity), este número se constituye como el DNI del teléfono móvil. Este número, que se asigna durante la fabricación, también es necesario para autorizar el uso del teléfono móvil a través de una red móvil.

Los proveedores de servicios de Internet cifran y mantienen segura esa información, pero en algunos casos raros pueden ser robados o mal utilizados (como en el caso de Facebook y Cambridge Analytica, donde millones de datos de usuarios han sido entregados a una empresa para hacer publicidad dirigida con fines políticos).

Aquí hay algunos consejos para ayudarlo con su identidad digital:

- Nombre de usuario: elija un nombre de usuario que lo represente claramente. Piense que podría estar usando esta dirección de correo electrónico para realizar trámites administrativos y que los nombres divertidos no siempre son bien aceptados. Su nombre de usuario estará delante del signo @ de su correo electrónico, por lo que nombres como “chicafacil@, chicoduro@, tupesadilla@” deben evitarse. Al elegir su nombre de usuario, no incluya números como su cumpleaños o los cumpleaños de sus seres queridos.
- Contraseña: utilice una combinación de letras minúsculas, mayúsculas, números y caracteres especiales como #, $, &, |, ~. Haga que tenga al menos 8 caracteres y cambie su contraseña con frecuencia. Si está accediendo a su cuenta digital a través de su teléfono móvil, use la huella digital u otra forma de autenticación. No "recuerde" la contraseña de su

cuenta en su navegador, es decir, el navegador de Google, por ejemplo, ofrece la posibilidad de guardar el nombre de usuario y contraseña de los sitios web a los que sueles entrar, como las redes sociales, para que no tengas que volver a introducirlos manualmente. Evita esto.

- Incluso si no es necesario, agregue explícitamente su teléfono móvil a su cuenta y configúrelo como el dispositivo predeterminado para recuperar las contraseñas olvidadas. Examine la configuración de su cuenta y configure el correo electrónico y el número de teléfono de recuperación para autenticar su identidad aún mejor. No use la misma contraseña para otras cuentas como las de redes sociales o juegos.

4. Cuestiones de seguridad y privacidad

Algunos servidores y aplicaciones pueden recopilar información extensa sobre un uso particular y, potencialmente, esta información se puede vincular a una persona física y sus hábitos digitales a través de Internet. A nivel de la UE, el GDPR (Reglamento general de protección de datos, aplicado en España a través de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales 3/2018) está tratando de lidiar con esto, pero aun así se recomienda a los usuarios que tengan cuidado de qué información y dónde comparten dicha información en Internet, especialmente cuando se trata de redes sociales.

Para procesar su contenido digital, existen numerosos editores de fotos y videos, mientras que las redes sociales también proporcionan capacidades de corrección ortográfica para textos escritos en inglés. En las fotos digitales (y videos) puede agregar diferentes filtros, cambiar la saturación, el contraste, etc. Puede usar los que se proporcionan con su dispositivo o instalar el que más le guste. Tenga en cuenta que la mayoría de los editores gratuitos en línea generalmente tienen algunas limitaciones, por lo que tiene que comprar la

versión de pago si quiere desbloquear todas las funciones. Esos servicios de software a menudo agregan a su foto o video una señal escrita, o marca de agua, de que el material ha sido creado usando este software, lo que puede no gustarle. Experimente y verifique hasta encontrar el que satisfaga sus necesidades.

Como se destacó en un estudio de la OCDE de 2016 "*Es imposible eliminar por completo el riesgo de seguridad digital cuando se realizan actividades que dependen del entorno digital. Sin embargo, el riesgo se puede gestionar, es decir, se puede reducir a un nivel aceptable a la luz de los intereses y beneficios en juego, y el contexto*". Sin embargo, hay pasos bastante razonables, y relativamente fáciles, que un individuo u organización puede tomar para alcanzar un nivel satisfactorio de seguridad digital y protección de la privacidad. Estos incluyen, entre otros, contraseñas seguras, una política estricta para el acceso online, sentido común en la navegación a través de Internet, educación y capacitación en los temas más comunes, la creación de una política sobre datos personales y la protección de datos personales. Dicho esto, la UE impone los más altos estándares de protección de los datos personales y de privacidad del mundo.

Como individuo, hay pasos sencillos para limitar la posibilidad de una violación de la privacidad. Por ejemplo, siempre se debe leer cuidadosamente la política de cookies de cualquier sitio web, servicio de internet, noticias y plataformas de redes sociales. En caso de que no desee ser rastreado (es decir, algunos sitios web recopilan datos sobre sus hábitos de navegación, con qué frecuencia visita un sitio web en particular, en qué anuncios hace clic, qué información busca en Internet, etc.) puede usar la navegación privada, también llamada de incógnito, que ofrecen casi todas las aplicaciones de navegación como Google Chrome, Mozilla Firefox, Internet Explorer de Microsoft, etc.

Por el lado de la seguridad, uno nunca debe usar las mismas contraseñas para diferentes aplicaciones de Internet, como el correo electrónico, las plataformas de redes sociales y sitios web que requieren iniciar sesión. Mantenga su contraseña segura con 10 o más caracteres, incluidos números, mayúsculas y

minúsculas y caracteres especiales como &, #, $, ^, etc. Como regla general, no guarde sus contraseñas en su navegador, pero trate de recordarlas o construirlas de acuerdo con una regla que haya formulado usted mismo. Por ejemplo:

#MiPrimerApellido4nombreSitioweb~mI_nOmbre$.

Aunque esto pueda parecer complicado, es fácil recordar la regla. Siempre que sea posible, agregue su teléfono móvil como alternativa de autenticación y recuperación de una contraseña olvidada o robada. Esto agregará una capa más de protección personal, lo que reduce el riesgo de uso malicioso de sus datos en línea.

5. Huella digital

La huella digital se refiere a las actividades digitales únicas y rastreables de un usuario en particular en Internet, es decir, el rastro que dejamos en Internet. El término también se puede encontrar como sombra digital, huella de Internet, sombra cibernética, etc. Aunque generalmente el término se aplica a personas físicas, también se puede usar para organizaciones, empresas, corporaciones, sitios de servicios digitales, etc.

Podemos distinguir dos tipos de huella digital:

- Huella digital pasiva: este término se refiere a los datos recopilados sin el conocimiento de la persona. Puede que no estos datos no hayan sido ocultados por el usuario.
- La huella digital activa: es la que el usuario comparte deliberadamente sobre sí mismo, generalmente en las redes sociales o en varios sitios web.

La información sobre el usuario puede ser dejada intencionalmente o no, y luego esta información es recopilada de manera activa o pasiva por otras partes. Por ejemplo, si en su perfil de redes sociales ha dejado visible su dirección de correo electrónico, su número de teléfono móvil, su domicilio, su lugar de trabajo, la dirección de Internet de su empresa, etc., será relativamente fácil para un

programa informático o una persona física recopilar gran cantidad de información sobre ti. En algunos casos, esta información también puede incluir sus cuentas bancarias o registros de impuestos, si se produce una violación de los registros de seguridad.

Se han realizado varios estudios que muestran que aproximadamente el 70% de todo el comportamiento digital de las personas es consciente y responsable. Sin embargo, aproximadamente el 30% de la huella digital de cada persona puede estar en una forma que nunca se habría revelado intencionalmente al público. Eso deja muchos datos para el análisis del comportamiento de compra, los hábitos de compra en línea, los pasatiempos y otras áreas de la vida personal. Si bien no hay nada de malo en los análisis de clientes en grandes bases de datos cuando se registran a los clientes o usuarios, tales análisis pueden ser objetivos para el robo de identidad, actividades criminales y violaciones de privacidad.

Si bien la huella digital no es una identidad digital o una identificación digital, el contenido y los datos descriptivos (también llamados metadatos) tienen un fuerte impacto en la privacidad, la confianza en Internet y la reputación digital. Las empresas pueden utilizar las huellas de Internet para reclutar personal nuevo, las agencias oficiales o del gobierno recopilan datos sobre usuarios específicos, los cuales no pueden recopilarse por otros medios, los vendedores siempre están buscando en qué tipo de productos están interesados los usuarios...

Las redes sociales son la fuente principal de dicha información. En algunos casos, las plataformas sociales pueden recopilar datos del dispositivo del usuario, incluso sin que el usuario lo sepa, utilizando varios sensores en los teléfonos móviles u otros dispositivos del usuario. Por ejemplo, Facebook y Google recopilan grandes cantidades de información del usuario que, si se combinan, pueden describir con bastante detalle la personalidad, intereses, opiniones políticas, hábitos de compra, intereses del usuario, etc.

6. Identidad Online

La identidad online es la identidad que el usuario elige construir en Internet, generalmente con fines de juego. Los usuarios pueden elegir representarse a sí mismos con avatares (gráfico del tamaño de un icono) en lugar de con sus fotos reales. Los usuarios también pueden usar seudónimos en lugar de sus nombres reales. Una identidad online puede incluso estar determinada por los enlaces del usuario al grupo de personas de Internet. Las identidades online están asociadas a usuarios reales a través de procedimientos de autorización como el registro y el inicio de sesión (nombre de usuario y contraseña), así como a través de la dirección IP específica de una máquina o dispositivo. Dichos sitios a menudo instalan cookies de seguimiento que pueden determinar el comportamiento online del usuario y vincularlo con una persona real. Como los juegos a menudo, pero no siempre, están dirigidos a un público más joven que no es tan cuidadoso en protegerse online, es crucial que la noción de identidad digital, identidad online y huella digital sea lo más clara posible para todos los que usan Internet.

La identidad online puede ser cualquier cosa, desde sus credenciales de correo electrónico (nombre de usuario y contraseña) hasta la cuenta de redes sociales, el nombre del foro o el perfil del comprador en un sitio web en particular. También incluye su historial de navegación, dirección IP, actividad de búsqueda, etc. Las personas y organizaciones pueden estar interesadas en su identidad online con fines totalmente legales o ilegales (piratas informáticos). Algunas de las empresas necesitan conocer su historial de navegación o historial de búsqueda para ofrecerle como publicidad productos o servicios más específicos, relacionados con sus necesidades e intereses. Otros podrían estar interesados en los objetivos ilegales de robar sus datos, número de tarjeta de crédito, etc.

Hay varias formas de proteger su identidad online, como contraseñas seguras, no compartir demasiados datos personales en las redes sociales, usar el modo de incógnito de su navegador, usar redes privadas virtuales, cifrar su comunicación, etc. Cuanta más atención pongas en tu identidad online, más segura será.

7. Resumen

En este módulo se ha introducido los conceptos básicos y el conocimiento necesario sobre la gestión de la identidad digital y la cuenta de Internet. Siguiendo esos conceptos clave, se ha descrito cuáles son los problemas de seguridad y la privacidad del usuario. Finalmente, se ha introducido lo que es una huella digital y una identidad online.

También se han propuesto métodos fáciles y comprensibles para crear contraseñas, autenticación, identidad digital, privacidad y navegación online. Una vez que un individuo u organización sigue las recomendaciones, pueden reducir los riesgos online en gran medida. Como siempre, no hay soluciones que cubran todos los casos y el sentido común, así como establecer políticas a nivel organizacional, ayudarán a combatir las acciones maliciosas online y aumentar la confianza en el uso de Internet y las plataformas digitales en su conjunto.

Finalmente, se ha tratado la identidad online y se ha señalado lo que cubre y cómo protegerse del uso ilegal de su identidad.

Bibliografía:

https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/

https://www.forbes.com/sites/forbestechcouncil/2019/06/07/a-beginners-guide-to-online-privacy-12-important-tips/#5092374e53ed

https://assets.mozilla.net/pdf/IHPbriefs_Online_Privacy_March_2017.pdf

https://www.commonsense.org/education/digital-citizenship/topic/digital-footprint-and-identity

https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1591780736&id=id&accname=guest&checksum=AF002079529F4DE263769B3FBEB40035