OBJETOS DE APRENDIZAJE

2019

LÍNEA 2

MATERIALES DE FORMACIÓN PARA ESTUDIANTES
DE GRADO DE LA COMPETENCIA DIGITAL

2. Comunicación y colaboración: 2.6. Gestión de la identidad digital: 4. Riesgos para la identidad digital

crue Universidades Españolas
Red de Bibliotecas REBIUN
Universidad Pontificia de Salamanca
Servicio de Biblioteca

Colección Objetos de Aprendizaje, 2019

MATERIALES DE FORMACIÓN PARA ESTUDIANTES DE GRADO DE LA COMPETENCIA DIGITAL

2. Comunicación y colaboración: 2.6. Gestión de la identidad digital: 4. Riesgos para la identidad digital

REBIUN Línea 2 (3er. P.E.) Grupo de Competencia Digital

crue Universidades Españolas Red de Bibliotecas REBIUN

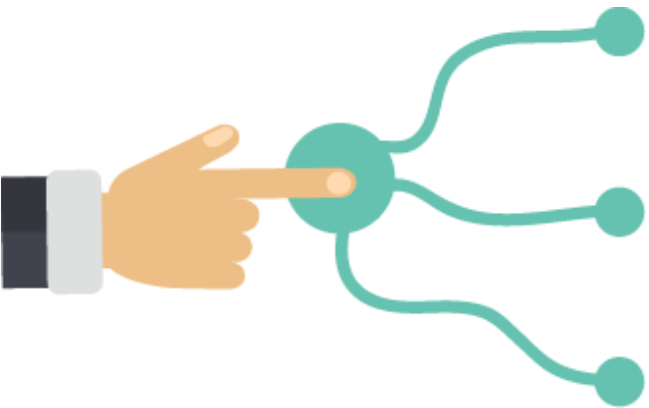
Comunicación y colaboración.
Gestión de la identidad digital

Riesgos para la identidad digital

CRUE REBIUN Red de Bibliotecas Universitarias

OBJETIVOS

Al finalizar esta actividad tienes que ser capaz de:



- Reconocer y controlar los **riesgos de robo de información personal**
- Reconocer y controlar los **riesgos de alteración de la identidad**
- Saber cómo **evitar dichos riesgos**

SUMARIO

- Robo de información personal
- Alteración de la identidad
  - Suplantación de identidad digital
  - Amenazas para la privacidad
  - Ataques a la imagen y a la reputación online
- Recomendaciones
- Para saber más...

RIESGOS FRECUENTES

1. ROBO DE INFORMACIÓN PERSONAL

Estos son algunos de los métodos para obtener datos de información personal:

- **Programas maliciosos (malware)** cuyo propósito principal es borrar, bloquear, modificar o copiar datos de los usuarios (virus, gusanos, troyanos…).
- **Phishing:** método utilizado para conseguir de forma engañosa (correo-e, llamadas telefónicas…) que se revele información personal (contraseñas, datos de tarjetas de crédito…)
- **Pharming:** práctica fraudulenta para redirigir un sitio web a otro falso, muy similar en apariencia, que instala software malicioso en el equipo del visitante o que inspecciona los datos personales del usuario.

RECOMENDACIONES

Si no quieres que te roben información personal...

- No abras ni leas correos electrónicos sin confirmar su procedencia y legitimidad.
- Introduce tus datos confidenciales solo en webs con protocolo seguro como https en lugar de http.
- No entres en webs con información privada (bancos…) a través de enlaces incluidos en correos electrónicos.
- No reveles tus claves y contraseñas a nadie y cámbialas con frecuencia.
- Mantén tu equipo protegido con antivirus.
- Evita utilizar redes Wi-Fi públicas para realizar operaciones privadas.

Ante la mínima duda, sé prudente y no te arriesgues

RIESGOS FRECUENTES

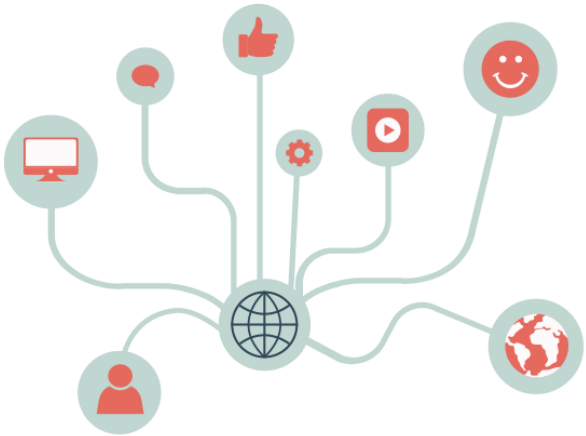
2. ALTERACIÓN DE LA IDENTIDAD

1. Suplantación de identidad digital
2. Amenazas para la privacidad
3. Amenazas a la reputación online

1 SUPLANTACIÓN DE LA IDENTIDAD DIGITAL

Se produce cuando alguien malintencionado se apropia indebidamente de la identidad digital de otra persona y actúa en su nombre. Puede hacerlo de varias formas:

- ✓ Registrando un perfil falso, sin utilizar información personal de la persona suplantada. Por ejemplo, perfiles caricaturizados de personajes públicos.
- ✓ Creando un perfil falso con datos de otra persona.
- ✓ Accediendo de forma no autorizada al perfil de alguien en un servicio de Internet para hacerse pasar por él.



2 AMENAZAS PARA LA PRIVACIDAD

Al participar en medios sociales pierdes el control sobre la difusión de la información que publicas y otras personas pueden hacer un uso inadecuado de la misma.
Estas son las principales causas que pueden suponer una amenaza para la privacidad:

- Configuración insuficiente de las opciones de privacidad del medio que utilizas
- Alteración de la privacidad derivada de la sincronización entre distintos medios
- Etiquetado en las redes sociales
- Sexting (envío de contenidos de carácter sexual a través del móvil)
- Uso de cookies sin conocimiento del usuario
- Compartir información que afecta a terceras personas

3 ATAQUES A LA IMAGEN Y REPUTACIÓN

El riesgo a sufrir un ataque al honor o a la reputación aumenta en Internet, ya que la viralidad en la difusión de los contenidos dificulta el control de la información personal por parte del propietario.
A continuación se exponen los principales motivos de amenaza a la imagen y a la reputación online:

- ✓ Impacto de las publicaciones que exceden a la libertad de información
- ✓ Daño reputacional debido a publicaciones falsas, injurias y calumnias
- ✓ Informaciones descontextualizadas
- ✓ Utilización no consentida de derechos de propiedad intelectual

RECOMENDACIONES

Debes aprender a configurar y revisar adecuadamente las opciones de seguridad y privacidad para garantizar al máximo el control de tu información personal

- Valora la información que publicas antes de hacerlo:
  - Sé especialmente cauto con las fotografías o vídeos que publicas en Internet, ya que te identifican físicamente.
  - Limita el uso de datos de localización a las aplicaciones estrictamente necesarias.
  - Adecua el grado de divulgación de tu información personal al tipo de relación con otras personas.

RECOMENDACIONES

- Configura bien los parámetros de privacidad y seguridad.
- Cierra adecuadamente la sesión en el perfil o servicio al terminar.
- Revisa periódicamente tus perfiles.

- Concede acceso solo a las aplicaciones de terceros que sean dignas de confianza:
  - Verifica al máximo quién es el titular de la aplicación a la que se autoriza el uso de datos de identidad, qué datos precisa y para qué los necesita.
  - Limita el acceso solo a los datos imprescindibles.

PARA SABER MÁS...

Consulta el capítulo 4 de la
Guía para usuarios: identidad digital y reputación online

Consulta el documento de la OCDE
At a Crossroads: Personhood and Digital Identity in the Information Society - OECD.org

Información sobre:
Regulación del derecho de rectificación


CRUE
REBIUN
Red de Bibliotecas Universitarias


UNIVERSIDAD PONTIFICIA DE SALAMANCA
Servicio de Biblioteca