Privacidad

Univisa S.A.
servclte@univisa.com.ec

Contenido

- **Privacidad**
- **Riesgos principales**
- **Cuidados a tener en cuenta**
- **Fuentes**

Privacidad (1/3)

- En Internet tu privacidad puede verse expuesta:
  - independientemente de tu voluntad
  - sin aviso o consentimiento previo cuando:
    - una persona:
      - divulga tus datos
      - divulga imágenes en las que apareces
    - un sitio web:
      - modifica sus políticas de privacidad
      - recolecta los hábitos y las preferencias de navegación de sus usuarios y las comparte con terceros
    - un impostor:
      - crea una cuenta o perfil en tu nombre y lo utiliza para hacerse pasar por ti

Privacidad (2/3)

- En Internet tu privacidad puede verse expuesta:
  - independientemente de tu voluntad
  - sin aviso o consentimiento previo cuando:
    - **un atacante o un software malicioso:**
      - **accede a los datos que ingresas usando el teclado**
      - **accede a datos que están almacenados en tu computadora**
      - **invade una de tus cuentas y accede a información restringida**
      - **invade una computadora en la que están almacenados tus datos personales**
      - **recoge datos que atraviesan la red sin estar encriptados**

Privacidad (3/3)

- En Internet tu privacidad puede verse expuesta:
  - independientemente de tu voluntad
  - sin aviso o consentimiento previo cuando:
    - **una aplicación instalada en tu computadora o dispositivo móvil:**
      - **recoge datos personales y los envía al programador/fabricante**
    - **el usuario:**
      - **comparte recursos de su computadora**
        - » **sin configurar restricciones de acceso adecuadas**
      - **utiliza contraseñas débiles**
        - » **que facilitan la invasión de sus cuentas**
      - **accede a sus cuentas desde computadoras potencialmente infectadas**
      - **no mantiene la seguridad de su computadora o dispositivo móvil**

Fuente - http://cartilla.cert.br/

Riesgos principales

Fuente - http://cartilla.cert.br/

Riesgos principales (1/2)

- **La divulgación y el uso indebido de los datos personales recogidos pueden:**
  - **comprometer tu privacidad, la de tus amigos y familiares**
    - **incluso cuando hay restricciones de acceso, no hay cómo controlar que una información no sea compartida con terceros**
  - **facilitar el robo de tu identidad**
    - **cuanta más información publiques más fácil será para un impostor crear una identidad falsa en tu nombre y usarla en actividades maliciosas, como:**
      - **acceder a sitios web**
      - **realizar transacciones financieras**
      - **enviar mensajes electrónicos**
      - **abrir empresas fantasmas**
      - **crear cuentas bancarias ilegítimas**

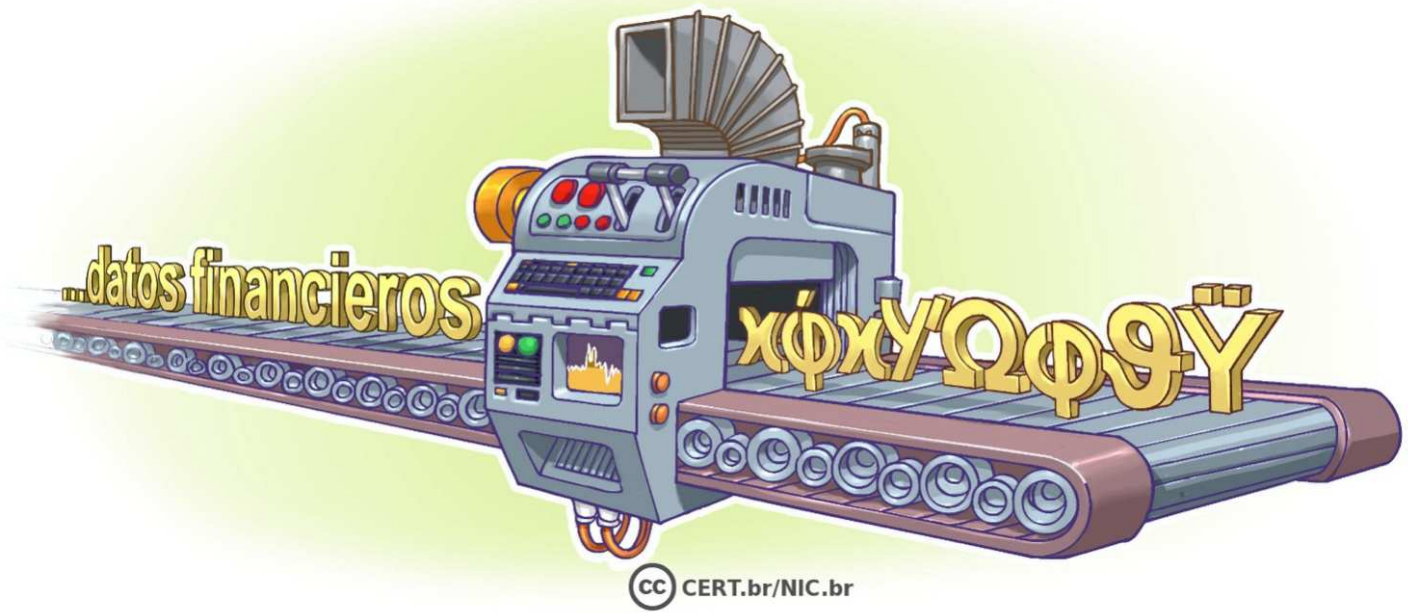
Fuente - http://cartilla.cert.br/

Riesgos principales (2/2)

- La divulgación y el uso indebido de los datos personales recogidos pueden:
  - facilitar la invasión de tus cuentas de usuario
    - las contraseñas y respuestas a las preguntas de seguridad pueden ser adivinadas si utilizas datos personales
  - posibilitar la publicidad dirigida
  - favorecer la recepción de spam
  - poner en riesgo tu seguridad física
  - provocar:
    - pérdidas financieras
    - pérdida de la reputación
    - acceso al crédito

Fuente - http://cartilla.cert.br/

Cuidados a tener en cuenta



Al acceder o almacenar correos electrónicos (1/2)

- **Configura tu programa de correo para que no abra imágenes que no estén contenidas en el propio mensaje**
  - **acceder a la imagen puede confirmar que el mensaje fue leído**
- **Utiliza programas de correo que permitan proteger criptográficamente tus mensajes**
  - **estos mensajes cifrados solo podrán ser leídos por quien logre decodificarlos**
- **Utiliza una conexión segura cuando accedas a tus correos a través de un navegador**
  - **esto puede evitar que tus mensajes sean interceptados**

Al acceder o almacenar correos electrónicos (2/2)

- **Almacena los mensajes confidenciales en formato encriptado**
  - **esto hace que sea más difícil que sean leídos por un atacantes o por un software malicioso**
  - **podrás decodificarlos cada vez que sea necesario**
- **Utiliza criptografía para la conexión entre tu lector de correos y los servidores de correo de tu proveedor**
- **Ten cuidado cuando accedas a tu *webmail***
  - **escribe la URL directamente en el navegador**
  - **clic en enlaces recibidos por medio de mensajes electrónicos**

Al navegar en la Web (1/2)

- **Ten cuidado al utilizar *cookies*:**
  - **Utiliza una o más de las siguientes opciones:**
    - **define un nivel de permisos igual o superior a "medio"**
    - **cambia tu configuración de modo que:**
      - **las *cookies* se borren al cerrar el navegador**
      - **no se acepten *cookies* de terceros**
    - **también puedes configurar tu navegador para que por defecto:**
      - **los sitios no puedan definir *cookies*:**
        - » **y luego crear una lista de excepciones, habilitando los sitios que consideras confiables y donde el uso de *cookies* es realmente necesario**
      - **los sitios puedan definir *cookies*:**
        - » **y luego crear una lista de excepciones, bloqueando los sitios no deseados**

Al navegar en la Web (2/2)

- **En caso que esté disponible trata de utilizar:**
  - **navegación anónima**
    - **principalmente al utilizar computadoras de otras personas**
    - **los datos sobre navegación no se verán amenazados**
  - **las opciones que indican que no deseas ser rastreado**
    - **"*Do Not Track*"**
    - **listas de protección contra el rastreo**

Al divulgar información en la Web (1/4)

- **Evalúa cuidadosamente la información que divulgas:**
  - **en tu página web, red social o blog**
  - **esta información puede ser usada para:**
    - **realizar estafas de ingeniería social**
    - **obtener tu información personal**
    - **atentar contra la seguridad de tu computadora**
    - **atentar contra tu seguridad física**
- **Piensa que estás en un local público**
- **Piensa bien antes de divulgar algo**
  - **después no es posible volver atrás**

Al divulgar información en la Web (2/4)

- **Publica la menor cantidad de información posible, tanto sobre tu persona como sobre tus amigos y familiares**
  - **aconséjales que hagan lo mismo**
- **Cada vez que alguien te pida información o al completar algún registro:**
  - **piensa si realmente es necesario que la empresa o persona tenga acceso a esa información**
- **Cuando recibas ofertas de trabajo a través de Internet:**
  - **limita la información disponible en tu currículum**
  - **solo proporciona más datos cuando estés seguro de que la empresa y la oferta son legítimas**

Al divulgar información en la Web (3/4)

- **Ten cuidado con los mensajes electrónicos en los que alguien te pide información personal o incluso contraseñas**

- **Ten cuidado al revelar tu ubicación geográfica**
  - **con esta información es posible averiguar tu rutina, deducir otros datos y tratar de anticipar tus próximos pasos**

- **Verifica la política de privacidad de los sitios que utilizas**
  - **trata de mantenerte al tanto de los cambios, en especial de los cambios relacionados con el tratamiento de los datos personales**

Fuente - http://cartilla.cert.br/

Al divulgar información en la Web (4/4)

- **Utiliza las opciones de de privacidad que ofrecen los sitios**
  - **trata de ser lo más restrictivo posible**
- **Mantén la privacidad de tu perfil y de tus datos**
- **Acepta tus contactos de forma selectiva**
- **Ten cuidado al unirte a un grupo o comunidad**

Fuente - http://cartilla.cert.br/

Al manipular datos y recursos

- Almacena la información sensible en formato encriptado
- Guarda copias de seguridad en sitios seguros y de acceso restringido
- Encripta el disco de tu computadora y tus dispositivos extraíbles
- Cuando utilices servicios de copia de seguridad (*backup*) en línea:
  - considera la política de privacidad y seguridad del sitio
- Cuando compartas recursos de tu computadora:
  - establece contraseñas para lo que compartes
  - comparte por el tiempo mínimo necesario

Fuente - http://cartilla.cert.br/

Cuentas y contraseñas

- **Ten cuidado al crear tus contraseñas**
  - **utiliza contraseñas largas y con diferentes tipos de caracteres**
  - **no utilices datos personales**
    - **nombre, apellido y fechas**
    - **datos que se pueden obtener fácilmente**
- **Evita reutilizar tus contraseñas**
- **No entregues tus contraseñas a otras personas**
- **Cuando utilices preguntas de seguridad:**
  - **evita escoger preguntas de seguridad cuyas respuestas se puedan adivinar fácilmente**

Fuente - http://cartilla.cert.br/

Computadora y dispositivos móviles

- **Mantén tu computadora o dispositivo móvil seguro**
  - **con las versiones más recientes de todos los programas instalados**
  - **instalando todas las actualizaciones**
- **Utiliza mecanismos de seguridad y mantenlos actualizados:**
  - ***antispam, antimalware y firewall* personal**
- **Al instalar aplicaciones desarrolladas por terceros:**
  - **ten cuidado al permitir el acceso a tus datos personales**
  - **verifica si los permisos necesarios son coherentes**
  - **escoge las aplicaciones de forma selectiva**
    - **escoge aplicaciones comprobadas y con un gran número de usuarios**

Fuente - http://cartilla.cert.br/

Mantente informado

Cartilla de Seguridad para Internet

http://cartilla.cert.br/

Fuente - http://cartilla.cert.br/

Fuentes

- **Fascículo Privacidad**

  http://cartilla.cert.br/fasciculos/

- **Cartilla de Seguridad para Internet**

  http://cartilla.cert.br/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil