Using Mobile Wallet?

Tips on How to Protect Your Information

As consumers increasingly use their mobile devices as wallets to do everything from paying for goods and services to banking, it's vital to protect your personal information.

Follow these eight simple tips to protect your information while using mobile wallet applications and services.

1. Choose apps or services from trusted sources. BEFORE you use them, read the privacy policies and terms and conditions to ensure you agree with them.

2. Use security features and software from your device manufacturer, carrier and/or app providers. This includes remote tracking, locking and erasing as well as passwords and PINS to prevent unauthorized access to your mobile device and to your mobile banking apps/services. These should be difficult to guess, changed periodically and never shared.

3. Choose a unique password that only works with your mobile wallet apps or services. Each one should be unique so that a cyberthief doesn't have access to all of your accounts.

4. Stay updated with your mobile device software and apps since these updates may contain improved security and enhancements.

5. Keep your Personally Identifiable Information (PII) such as name, address or birth date and credentials (e.g., login username) private and secure.

6. Only connect to knowingly secure networks, such as your carrier's network. Most free Wi-Fi hotspots are unsecure, which make you more vulnerable to hackers and cyberthieves.

7. Back up the information on your mobile device to a PC or service provider (e.g., cloud) in the event it needs to be restored or downloaded to a new device.

8. In the event something goes wrong, know who to contact so you may stop any unauthorized use or purchases ASAP.

For more tips on how to keep your information safe, please visit: http://ctia.it/ST7xir

Last Updated: May 2013

CTIA
The Wireless Association®

¿Usa una billetera móvil?

Consejos para proteger su información

Como los consumidores usan cada vez más sus dispositivos móviles como billeteras para hacer todo, desde pagar bienes y servicios hasta realizar operaciones bancarias, es vital proteger su información personal.

Siga estos ocho simples consejos para proteger su información cuando utiliza aplicaciones y servicios de billetera móvil.

1. Elija aplicaciones o servicios de fuentes confiables. ANTES de usarlos, lea las políticas de privacidad y los términos y condiciones para asegurarse de estar de acuerdo.

2. Use funciones de seguridad y el software del fabricante o proveedor de su dispositivo, o de los proveedores de aplicaciones. Esto incluye rastreo, bloqueo y borrado remotos, como también contraseñas y números de identificación personal (PINS, por sus siglas en inglés) para evitar accesos no autorizados a su dispositivo móvil y a sus servicios/aplicaciones de banca móvil. Estos deben ser difíciles de adivinar, deben modificarse periódicamente y nunca deben compartirse.

3. Elija una contraseña única que funcione sólo con las aplicaciones o los servicios de su billetera móvil. Cada contraseña debe ser única para que, en el caso de que le roben, un ladrón cibernético no tenga acceso a todas sus cuentas.

4. Actualice periódicamente el software y las aplicaciones de su dispositivo móvil, ya que estas actualizaciones pueden incluir mayor seguridad y otras mejoras.

5. Mantenga su información de identificación personal (PII, por sus siglas en inglés) como nombre, dirección o fecha de nacimiento y credenciales (por ej., nombre de usuario de inicio de sesión), como información privada y segura.

6. Conéctese solo a redes seguras, como la red de su proveedor. La mayoría de las zonas con conexión inalámbrica gratis por red Wi-Fi no son seguras, lo que lo hace más vulnerable a los piratas y ladrones informáticos.

7. Haga una copia de seguridad de la información en su dispositivo móvil en una PC o en un proveedor de servicio (por ej., nube) en el caso de que necesite restaurarla o instalarla en un dispositivo nuevo.

8. Si algo sale mal, sepa a quién debe contactar para interrumpir inmediatamente cualquier uso o compras no autorizados.

Para obtener más consejos sobre cómo mantener su información segura, visite: http://ctia.it/ST7xir.