bank's contact number or short code in your address book so you'll see its name when you get a legitimate email or text message. And don't respond to text, email or other requests for your password or other private information, even if the sender claims to be someone you do business with.

Avoid landing on a spoofed website—a copy of a legitimate site designed to lure you into revealing your password and other sensitive information—by bookmarking your bank's website while on the legitimate site. (You'll avoid the possibility of mistyping the Web address, or URL.) Don't go to the site by clicking a link in an email or text message.

Download apps only from trusted sources. If the source is unknown, do an online search for reviews and user feedback to find out if others have had problems with the app. (Lookout Mobile Security (www.mylookout.com/about), a free app for Blackberry and Android phones, checks apps for malware, spyware and viruses.) Before using a new app, look into its policy regarding disputed or unauthorized transactions.

Use your wireless carrier's network rather than public (non-passworded) Wi-Fi for shopping or banking. Check for "https" instead of just "http" in the Web browser address bar, which indicates the site is secure and encrypted.

Confirm before making a payment or purchase that you will get a receipt. Keep your receipt until you receive, and are satisfied with, your purchase.

Monitor the activity on your accounts regularly—even weekly or daily. You'll detect fraud sooner rather than later. And, in most cases, you must report unauthorized account activity within a certain time period (say, within 60 days of when the transaction posted) to be protected by a zero liability guarantee. Your wireless carrier and other payment processors all have policies for disputing unauthorized charges to your account, but not all companies offer zero liability. Generally speaking, you'll get the strongest liability protection with the fewest hassles when you use a credit or debit card with a zero liability policy.

Know how long it takes for your transactions to be processed so that you correctly time your payment requests, deposits and other activity.

Contact your wireless provider immediately if you lose your phone, to suspend your service. Then log on to your financial accounts on a computer and deactivate text banking and change your passwords. (Call your bank if you need help.)

Many of the practices for safe mobile banking are the same as those recommended for secure online banking. *(Learn more in the "Digital Dollars" companion brochure "Banking online safely," available at www.consumer-action.org.)*

Though it's not an issue of safety, be aware that mobile banking activity may cost you money in higher wireless service bills. If so, consider online banking from your home computer or inquire about other service plans that better accommodate your usage.

Assistance

Whether you're already a mobile banking customer or just getting started, you can contact your financial institution's customer service department directly for guidance. Likewise, contact the app vendor or the merchant regarding any mobile payment questions or issues.

If you're dissatisfied with a purchase, try first to resolve the issue directly with the seller. If you aren't able to come to an agreement and you want to dispute a payment, contact the credit card company or financial institution that issued the card you used to make the purchase.

If your payment was processed through an intermediary, such as an Internet payment service account or your wireless service provider, follow that company's instructions for filing a dispute.

Learn more

Learn more about staying safe while using mobile and Web-enabled devices:

OnGuard Online: ***www.onguardonline.gov***

The U.S. federal government and the technology industry provide information and tips for online safety and security.

Privacy Rights Clearinghouse: ***www.privacyrights.org***

The nonprofit Privacy Rights Clearinghouse offers a library of information, from tips for protecting your privacy online to how to shop safely on the Internet.

Consumer Action

www.consumer-action.org

Consumer advice and referral hotline:

hotline@consumer-action.org or 415-777-9635

Chinese, English and Spanish spoken

Consumer Action created the Digital Dollar series with funding from Visa Inc.

VISA   consumer action
Education and advocacy since 1971

Visit Visa's financial education program, Practical Money Skills, at: *www.practicalmoneyskills.com*

Your Digital Dollars

Mobile banking and mobile payments

Make financial transactions safely on the go

Financial education from *Consumer Action and Visa Inc.*

Check your balance...transfer money...make a purchase—these are just a few of the things you can do on the go with a cellular telephone or other mobile device.

There are a lot of benefits to being able to bank or make payments from just about anywhere, but it's important to know how to do these things safely. Understanding the types of transactions that are possible on a mobile device, the potential risks of banking and paying on the go, and how to keep your personal information, money and credit safe can help you get the most out of mobile technology.

What is mobile banking?

Mobile banking allows you to access your financial accounts and conduct transactions wirelessly, using your mobile device. Most major financial institutions, including banks, credit unions, lenders and investment companies, offer mobile banking. Increasingly, smaller financial institutions also offer mobile banking.

What you can do using a mobile device depends on the technology used by the bank, your wireless service plan and the type of phone, smart device, tablet computer or PDA (personal digital assistant) you have. You need a smartphone with data service or Internet access to take advantage of the most advanced mobile banking capabilities. Before you can access accounts on your mobile device, you may be required to complete the enrollment and setup process on a computer.

There are three types of mobile banking that your bank may offer:

- Text, or SMS (short message service). Text banking allows you to get information about your account (such as your balance) and receive information and alerts via text message. It's possible from any cell phone that supports texting, but usually you can't conduct transactions.
- Online banking via mobile device. You log on to your bank account using your mobile device's Web browser, just like you would on a laptop or desktop computer. It enables you to do all the same things you can do with online banking. This requires a Web-enabled device and a data service plan.
- Mobile banking applications. "Apps" are specially designed programs that are downloaded and installed on a smartphone, tablet or PDA. Apps typically are faster to use and easier to navigate on a small screen than a website is, and they allow you to conduct the full range of transactions. (Some banking apps even allow you to make a deposit by taking a picture of the front and back of the check!) To use a mobile banking app, you must have an advanced mobile device with Wi-Fi or a data service plan.

What are mobile payments?

Mobile payments are payments you make using your mobile device, instead of writing a check, handing over cash or pulling out a credit or debit card.

There are many types of mobile payments:

Mobile Web payments allow you to make purchases remotely, when shopping on your mobile device via a downloaded app or your Web browser. The purchase amount typically is charged to a credit or debit card, a pre-registered Internet payment service account or a "digital wallet" (a program that stores your payment and shipping information for Internet and electronic transactions).

Mobile text (SMS) payments allow you to make purchases via text message. This is sometimes called "text to buy." The transaction might be added to your wireless service bill or charged to a pre-registered credit or debit card, Internet payment service account or digital wallet. This type of mobile payment typically is used for small amounts, such as the cost of downloads (ringtones and songs, for example), parking fees, transportation fares and movie tickets, though it is even possible to authorize a payment to family members in another country by text message or buy big-ticket items from certain retailers.

Direct mobile billing (less common) allows you to have purchases added directly to your wireless service bill at checkout if the option is available.

Mobile peer-to-peer (P2P) payments are typically small, informal transactions between two people—for example, paying a handyman or covering part of a dinner bill. The payment may be made using an app or, less common, by touching two smartphones together.

Mobile point-of-sale payments (also known as proximity payments) make it possible to make purchases at the cash register or other point of sale simply by tapping or waving your mobile device close to an electronic reader. This payment option is becoming more widely available as more phone manufacturers and merchants install the necessary chips and chip readers.

What to know

Making purchases and banking by mobile device isn't particularly risky, but that doesn't mean that it's absolutely risk-free. It's important for anyone who uses mobile banking and payment technology to be aware that:

- It's possible to lose access to your accounts if you're outside your wireless service coverage area or your phone battery is dead. Bill payments could be late if you can't get service in time to place the payment request. (This is a great reason to pay bills early whenever possible!)
- It's far more likely that you would lose your mobile device than, say, a desktop computer. A lost phone would not only be inconvenient, it could leave your personal data, account information and purchase ability accessible to someone who finds it. *(See "Safety tips.")*

> ***TIP:*** *Anytime you send sensitive information over an unsecured wireless network, it could be exposed.*

- Though not a major issue so far, malware (viruses, spyware and other code designed to steal your information or do harm to your device or data) could hit phones more widely in the future. Antivirus and firewall protection is not yet widely available for mobile devices.
- Mobile banking could cost you money if you pay for service per unit (text message or megabyte of data), if you use more text messages or data than is included in your monthly service plan or if you use your service while roaming outside your carrier's network.

Safety tips

Financial institutions, card issuers, major retailers, payment networks, wireless service providers, etc. work hard to make mobile banking and mobile payments safe and problem-free. Still, there are things you can do yourself to protect your information, accounts and mobile device.

Guard your mobile device like you would your wallet, since it may contain information that someone could use to make purchases or access your accounts. Don't lend your phone to anyone you don't know and trust. Find out if there is a way to delete the device's contents remotely if it's lost or stolen. (There are many software products available that help owners locate missing devices or remotely "wipe" personal data from the phone.)

Create strong passwords for both your device (to turn it on or wake it up from sleep mode) and all your banking and payment apps. They should be at least eight characters long and use a combination of uppercase and lowercase letters, numbers and symbols. Don't share your passwords, personal identification numbers (PINs), usernames or the answers to "password hints" with anyone. Don't use the "Remember me" function or similar options to store passwords or payment information on sites or in apps. Change your password regularly; change it immediately if you think it's been compromised.

Log off and close the browser window or the app when you're finished. Turn off Bluetooth devices that link to your phone when you are not using them. Lock your phone when not in use.

Don't send sensitive information via email or instant message (IM), since these aren't automatically encrypted. Keep your