Online banking via mobile device. You log in 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 or Wi-Fi.

Mobile banking applications. “Apps” are specially designed software programs that are downloaded and installed on a smartphone or tablet. 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. (Most 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:

- **Proximity mobile payments** (also known as NFC—Near Field Communication—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 is done through the smartphone’s contactless payment function—Apple Pay or Google Pay, for example.

- **Mobile web payments** allow you to make purchases remotely, whether on your device via your mobile web browser or the retailer’s app. The purchase amount typically is charged to a credit or debit card number you enter or to a pre-registered online payment service account (or digital wallet), such as PayPal.

- **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—made using a mobile payment app (Venmo, Zelle or PayPal, for example).

- **SMS payments** (also known as “text to pay” or “pay by text”) allow you to make purchases via text message. The transaction might be added to your wireless service bill or charged to a 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.

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

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 if 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 is more likely to be lost or stolen than, say, a desktop computer. A lost phone is more likely to be lost or stolen.

- Anytime you send sensitive information over an unsecured wireless network, it could be exposed. (This is a great reason to pay bills early whenever possible.)

- Malware (malicious code designed to steal your information or do harm to your device or data) can hit phones just as they can computers. Precautions need to be taken to minimize the risk.

- Malicious software programs that are downloaded and installed on a smartphone or tablet and 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 bank’s contact number or short code in your address book so you’ll see its name when you get a text message 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 "spoof" website—a copy of a legitimate site designed to lure you into revealing your password and other sensitive information—by bookmarking your frequently used banking, payment and shopping websites 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. Before using a new payment, banking or shopping 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 your transaction is confirmed or 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, financial institution 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 stronger liability protection with a credit or debit card than with a prepaid card.

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 carrier immediately to suspend your service if you lose your phone. Then log in 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 https://www.consumer-action.org/modules/articles/your_digital_dollars-banking_online_safety.)

Though it’s not an issue of safety, be aware that mobile banking and payment activity may cost you money in higher wireless service bills. If so, consider online banking and payments 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 online payment service provider, 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. (Learn more in Consumer Action’s Savvy Online Shopping publications: https://www.consumer-action.org/modules/module_online_shopping.)

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

Learn more
Learn more about staying safe while using mobile 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 non-profit 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:
https://complaints.consumer-action.org/forms/english-form or 415-777-9635
Chinese, English and Spanish spoken
Consumer Action created the Digital Dollar series with funding from Visa Inc.

Visit Visa’s financial education program, Practical Money Skills, at: https://www.practicalmoneyskills.com

© Consumer Action 2011
Rev. 3/20