Your Digital Dollars

Online and mobile banking and mobile payments

Lesson Plan and Class Activities

A Consumer Action Training Guide

Your Digital Dollars:
Online and mobile banking and mobile payments

Lesson Plan and Class Activities

A Consumer Action Training Guide

Lesson Purpose:

To make participants aware of how online and mobile banking and mobile payments work, to help them understand what the advantages and disadvantages of banking or paying electronically might be, and to provide them with the knowledge and tools that will enable them to protect their assets and their privacy while banking and paying online and on the go.

Lesson Objectives:

By the end of the lesson, participants will understand:

- what online banking, mobile banking and mobile payments are.
- what sorts of transactions are possible, who offers online and mobile banking and payment services, and what tools and information are needed to be able to bank or pay digitally.
- what the various online and wireless banking and payment platforms are and what capabilities are available with each.
- the benefits and risks associated with banking and paying digitally.
- how to protect their personal information, device data and accounts.
- what to look for in financial institutions, online merchants and mobile app providers.
- how to enhance the security of every online or mobile transaction.
- what resources are available to provide additional information and assistance.

Lesson Duration:

2½ hours (plus a 10-minute break)

Materials:

For instructor:

- Brochures:
  - *Banking online safely: Protect your identity and accounts while banking by computer*
  - *Mobile banking and mobile payments: Making financial transactions safely on the go*
  - *Safety and privacy in online and mobile transactions: Protect your identity and data while banking or paying digitally*
- Lesson plan (pages 3-16)
- Activities (including answer keys) (pages 17-22)
  - What's "Phish-y" About This? (pages 17-20)
  - Mobile Banking and Payment Safety (pages 21-22)
- Evaluation form (page 23)
- Visual teaching aid (PowerPoint presentation with instructor's notes)

Instructor will also need:

- a computer and projector for the PowerPoint presentation (optional). (The PowerPoint slides also can be printed on transparent sheets for use on an overhead projector.)
- an easel and pad, or a whiteboard, and markers.

For participants:

- Brochures:
  - ***Banking Online Safely:*** *Protect your identity and accounts while banking by computer*
  - ***Mobile Banking and Mobile Payments:*** *Making financial transactions safely on the go*
  - ***Safety and Privacy in Online and Mobile Transactions:*** *Protect your identity and data while banking or paying digitally*
- Activities:
  - What's "Phish-y" About This? (2 pages)
  - Mobile Banking and Payment Safety (1 page)
- Evaluation form (1 page)
- OPTIONAL: Printout of the PowerPoint presentation

Lesson Outline

- Welcome (5 minutes)
- Online Banking (10 min)
- Mobile Banking (10 min)
- Mobile Payments (15 min)
- What to Know About Digital Banking and Payments (10 min)
- Activity: What's "Phish-y" About This? (15 min)
- Break (10 min)
- Protecting Your Mobile Device and Data (10 min)
- Online Banking Precautions (10 min)
- Vetting Financial Institutions, Online Merchants and App Providers (5 min)
- Avoiding Scams, Fraud & Malware (10 min)
- Guarding Your Data (10 min)
- Activity: Mobile Banking and Payment Safety (15 min)
- Assistance & Resources (10 min)
- Questions & Answers (10 min)
- Wrap-up and Evaluation (5 min)

Financial education from Consumer Action and Visa Inc.

Instructor's Notes:

This "Your Digital Dollars" training module, consisting of three brochures (*Banking Online Safely: Protect your identity and accounts while banking by computer; Mobile Banking and Mobile Payments: Making financial transactions safely on the go; and Safety and Privacy in Online and Mobile Transactions*: *Protect your identity and data while banking or paying digitally*), a lesson plan that includes class activities, and a PowerPoint presentation, was created by the national non-profit organization Consumer Action in partnership with Visa to be used nationwide by non-profit organizations providing personal finance, consumer and housing education in their communities.

Before conducting the training, familiarize yourself with the three brochures, the lesson plan (including activities), and the PowerPoint visual teaching aid.

The PowerPoint presentation contains notes for each slide (appearing below the slide when in Normal view or Notes Page view, and inserted into the lesson plan). These notes offer detailed information about the items appearing on the slide. The lesson plan includes indicators so you will know which slide corresponds to each part of the lesson, and when to move to the next one.

Why Adults Learn, a PowerPoint training for educators, provides tips for teaching adults and diverse audiences—it will be helpful to you even if you have taught similar courses before. The slide deck is available at the Consumer Action website (http://www.consumer-action.org/outreach/articles/why_adults_learn/).

Welcome (5 minutes)

➡**SLIDE #1** (onscreen as participants arrive; direct participants who arrive early to beginning reading the three brochures)

Welcome participants. Introduce yourself and present the purpose of the training and the agenda.

Review the contents of participants' packets. Ask the class to take a look inside their packets and make sure they have all the materials needed.

If you have a small group, you can ask individuals to introduce themselves and tell you what they hope to get out of the training. In a larger group, invite volunteers to share their expectations. On your whiteboard or easel pad, jot down some of the specific things participants mention. You can come back to this at the end of the training to make sure you've covered these points. (This activity is designed to serve as a brief icebreaker. It will also give you an idea what participants' expectations and needs are.)

Ask: When is the last time you saw a line *inside* a bank branch (not at the ATM!), or the last time you wrote a check for an everyday purchase? Fewer customers visiting the bank and fewer checks changing hands are just two signs that more consumers are using technology to manage their finances and make purchases. Today we'll be learning about:

- how you can do your banking online or on your mobile device;
- the different types of financial transactions that are possible with a mobile device;
- the advantages and disadvantages of banking and paying electronically; and,

- how to protect your assets and your privacy while banking and paying online and on the go.

Online Banking (10 minutes)

Introduction: Online banking is sometimes referred to Internet banking or e-banking. It makes it possible for you to access your financial accounts and conduct certain transactions using your computer and a high-speed, or broadband, Internet connection.

Ask: *What kinds of banking tasks can you do online?* (Allow time for responses. You can jot them down on your easel or whiteboard, if you like.)

➡SLIDE #2

Go over slide bullet points, referring to slide notes for further explanation/examples for some of the items:

- Being able to search for transactions by date, amount, check number or other criteria is useful if you need proof that you made a payment or deposit.
- Being able to view canceled checks is useful if you forgot to enter the check in your check register and can't remember whom it was made out to.
- To use online bill-pay services, you enter payee information (name, address and account number) and the amount of the payment. The payee stays in your list to be used monthly or as needed. You can set up automatic recurring payments, too.
- Account terms include such things as interest rate and payment due dates for loans (when you are on, say, your mortgage lender's site or the site of the lender who has your auto loan).
- Alerts are text or email messages that notify you of certain account activity or status. For example, you might choose to get an alert when your account balance drops below a certain amount, when a direct deposit is made to your account, or when a check clears.

Ask: *What kinds of alerts would you find helpful in managing your money, your bank accounts and your bills?* (Different financial institutions offer different types of alerts, and many credit card issuers, phone service carriers, lenders, and others also offer alerts that notify you, for example, when your new statement is ready, when the bill is due, when you are approaching your limit, and more.)

➡SLIDE #3

Go over slide bullet points.

After reading the last bullet point, ask: *Would you feel comfortable putting your money in a bank that offered only online access, and did not have branches you could visit?* (Allow a moment for class input.)

Explain that there are a number of reputable banks that operate only online. Since these banks have lower overhead costs (no branches to open, maintain and staff), they often pass those savings on to customers in the form of no or lower fees and/or interest paid on the account. If you're interested in an Internet-only account, look for one that waives or reimburses some or all the fees you'll be charged for using other banks' ATMs. And, if you plan to make check deposits

(instead of direct deposit), make sure the bank offers an app that allows you to do so by taking a photo of the check with your smartphone. This is not a good option for customers who have to deposit cash.

➡SLIDE #4

The online banking process is pretty similar regardless of which financial institution you have your account at.

Go over slide bullet points, referring to slide note:

- You must register before you can begin banking online. That entails setting up your login information, which typically is either a username you create or your email address, and a password you create. If you have more than one account with the institution, you will be given the option to select the one you want to work with now.

Ask: *What are the advantages of being able to do your banking online?* (Allow time for responses. Jot down answers on your whiteboard or easel.)

➡SLIDE #5

Go over slide bullet points, referring to slide notes:

- Banking anytime, anywhere, as long as you have Internet access and a computer.
- Direct deposit is safer, faster and more convenient than handling a physical check. Cash can be gotten from an automated teller machine (ATM) or as part of a debit card purchase (at the grocery store, for example, by requesting “cash back”).
- Savings include the cost of stamps to mail bills, the cost of checks, and the cost (in time and gas) of trips to the bank, post office or mailbox.
- Checking your account frequently online is not only convenient, it’s a good way to spot any errors or signs of fraud sooner rather than later. And it can help you avoid overdrawing your account.
- Many e-accounts—accounts that require transactions be conducted online or at the ATM—are fee-free or charge only a small monthly fee.
- Online banking is green: no paper account statements, and you may also be able to sign up to receive e-bills; fewer or no checks and envelopes; and, no gas used for trips to the bank, post office or mailbox.

Mobile Banking (10 minutes)

Introduction: Mobile banking is sometimes referred to as m-banking. It makes it possible for you to access your financial accounts and conduct transactions wirelessly, using your mobile device. It’s no longer impossible to deposit a check while sitting on a beach or to pay the electric bill while sightseeing halfway around the world.

Ask: *What kinds of banking tasks can you do using a mobile device?* (Allow time for a few responses.)

➡SLIDE #6

Go over slide bullet points, referring to slide note:

- Exactly what you are able to do from a mobile device depends on the type of phone, smart device, tablet computer or PDA (personal digital assistant) you have; your wireless service plan; and the technology used by the financial institution. A smartphone with data service is required to take advantage of the most advanced mobile banking capabilities.

➡SLIDE #7

Go over slide bullet points, referring to slide notes:

- Banking by text message is limited to getting information about your account (such as your balance) and receiving text alerts.
- Online banking via mobile device is similar to online banking via computer: You use the device's Web browser to log in to your account, and then you can conduct all the same transactions as you can on your computer.
- An app typically is faster to use and easier to navigate on a small screen than a website.

Mobile Payments (15 minutes)

Introduction: Mobile payments, or m-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.

Ask: *Have any of you ever made a payment or purchase with your mobile phone or PDA? Where was it? What did you like about it?* (Allow time for a few responses.)

➡SLIDE #8

Go over slide bullet points, referring to slide notes:

- When shopping using an app or the Web browser on your mobile device, the purchase amount typically is charged to a credit or debit card, a pre-registered Internet payment service account (such as PayPal) or a "digital wallet" (a service that stores your payment and shipping information for electronic transactions).
- Sometimes called "text to buy," a text (SMS) 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 to 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.
- P2P payments are typically small, informal transactions between two people—for example, paying the gardener or covering your share of a dinner bill. The payment may be made using an app or, less common at this point, by touching two smartphones together.

- Proximity (indicating “close”) payments make it possible to make purchases at the cash register or other point of sale (POS) 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.

Review of banking and payment types:

➡SLIDE #9

Read each statement and have participants identify which type(s) of banking or payment type the statement describes—there may be more than one correct answer to each item. You can call on volunteers or invite the class to call out responses.

1. I can check my balance 24/7. (online banking and all types of mobile banking—text/SMS, mobile Web browser and mobile app)

2. My banking capabilities are limited. (text (SMS) banking)

3. I can pay my bills anytime. (online banking, mobile Web and mobile app)

4. My banking activity could cost me money. (any type of mobile banking if you exceed the text or data service included in your regular monthly wireless service plan)

5. I bought a new sweater using my mobile phone. (mobile Web payment)

6. I paid for my coffee by waving my mobile phone near a machine. (mobile point-of-sale (POS/proximity) payment)

7. I paid my babysitter. (mobile peer-to-peer (P2P) payment)

8. I entered a code and purchased a new ringtone. (mobile text (SMS) payment, or “text to buy”)

9. I bought something and the charge was added to my wireless bill. (direct mobile billing or, possibly, mobile text (SMS) payment)

10. I can deposit a check by taking a picture of it. (mobile app banking)

11. I have to sign out or log off to end this type of banking session. (online, mobile Web and mobile app)

12. I have to visit the financial institution’s website. (online banking and mobile Web banking)

13. What I can do depends on the type of device I have. (mobile banking and mobile payments—text banking and text payments are the only two that are possible with virtually any device)

14. I have to complete the enrollment and setup process on a computer. (online banking and mobile Web or mobile app banking)

15. I need to download a special program first. (mobile app banking)

16. This type of banking can be done using virtually any mobile phone. (text (SMS) banking)

17. This type of banking requires an Internet connection. (online, mobile Web and mobile app)

18. I may be able to send money to my family back home by entering a code. (mobile text (SMS) payment)

19. I can make these types of payments using a digital wallet. (mobile Web, mobile text (SMS) and mobile peer-to-peer)

What to Know About Digital Banking and Payments (10 minutes)

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

Ask: *What do you think some of the potential risks or issues could be when banking and paying online or wirelessly using a mobile device?* (Allow time for a few responses. Write responses on whiteboard or easel, if you like.)

➡SLIDE #10

Go over slide bullet points, referring to slide notes:

- It's possible to temporarily lose access to your accounts if you're outside a wireless coverage area, your phone battery is dead, you don't have access to a computer, the Internet connection is interrupted or the institution's system is "down."
- Bill payments could arrive late because there is not enough time between when you request the payment and when the bank makes the electronic transfer or mails the check.
- 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.
- Anytime you send sensitive information over an unsecured wireless network there's the possibility that it could be exposed.
- Your personal data or your accounts could be accessed without your permission as the result of a data breach (the theft or unintentional release of information held in an institution's database) or because someone has obtained your username and password.
- Your computer could become infected with malware (viruses, spyware and other code designed to steal your information or do harm to your device or data). Though not a major issue for mobile devices so far, malware could hit phones more widely in the future. Antivirus and firewall protection is not yet widely available for mobile devices. Or you could become the victim of a phishing attempt (trying to get you to reveal your password or other sensitive data) or other scam (such as a "spoofed" website).
- It's possible that your information could be collected and used for marketing purposes or sold to a third party. This could result in nuisance email messages, pop-up windows and other annoying marketing efforts.

- If you pay for wireless service per unit (text message or megabyte of data), or 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 carriers' network, the activity on your mobile device could increase your monthly service bill.

Activity: What's 'Phish-y' About This? (15 minutes)

➡SLIDE #11

Have participants remove the *What's "Phish-y" About This?* activity from their packets.

This activity can be done individually or in small groups. Instruct participants to circle any "red flags"—things that tip them off that the message is phishing for personal information or the website could be "spoofed."

Allow 5 to 10 minutes to complete the activity.

If the activity was completed individually, invite participants to raise their hands if they would like to answer. If the activity was done in groups, rotate among them, giving a spokesperson from each group the opportunity to answer when it is that team's turn.

Refer to the answer key provided for the list of red flags and additional information.

Break (10 minutes)

Announce a 10-minute break. Make yourself available for a few minutes to direct people to the restroom or a place to get drinks and snacks.

Leave the following slide onscreen during the break.

➡SLIDE #12

Protecting Your Mobile Device and Data (10 minutes)

Introduction: The more you do online or on your mobile device, the more opportunity there will be for your personal data to be unintentionally exposed, stolen or misused. You can greatly reduce the odds of that happening by being careful, and by taking steps and using tools to enhance security.

➡SLIDE #13

Depending on how you use your mobile device, it might be less like a phone and more like a wallet that can make calls. Since your mobile device may contain information that someone could use to make purchases or access your accounts, it makes sense to put extra effort into keeping it safe and secure.

Go over slide bullet points, referring to slide notes:

- Don't leave your mobile device unattended or accessible to anyone else. Don't lend your phone to anyone you don't know and trust.
- Old text messages that contain online banking or purchase/payment transaction messages that you would not want someone else to see could still reside on your

device. (This information may also be saved on your computer if you "sync" your phone with your computer.) Delete sensitive messages regularly.

- Don't save your account numbers or access information anywhere on your mobile device where someone could get to it.
- Use a password to lock the phone when it's not being used, and set the phone to automatically lock after a certain number of minutes of being idle.
- There are many software products available that help owners locate (track) their missing device or "wipe" their data remotely if the device is ever lost or stolen.
- If you lose your phone, contact your wireless service carrier immediately to suspend your service. Then use a computer to log on to your financial accounts and deactivate text banking, change passwords and otherwise secure your accounts. (You also may be able to do this by calling your bank.)
- This entails more than just deleting files. Check the "help" menu or the manufacturer's site for instructions, or contact your wireless carrier for help with a phone or PDA.

Online Banking Precautions (10 minutes)

Introduction: Financial institutions put a great deal of effort into making online banking and other online transactions as secure as possible. But there's a lot you can do *yourself* to increase the likelihood that your personal information will remain private and your accounts will stay off limits to others.

Ask: *What sorts of things could you do to make your online banking experience problem-free?* (Allow time for responses, before revealing the next slide.)

➡SLIDE #14

Go over slide bullet points, referring to slide notes:

- If there's any doubt in your mind about the legitimacy of the financial institution, take the time to check it out before you put your money there. Read about the bank in the site's "About Us" section, and then try to verify the information. For example, call the phone number provided. Also, do an online search to find any posts about the institution, including consumer complaints. Don't be fooled by a fancy website.
- Confirm that the institution is insured by the Federal Deposit Insurance Corporation (up to $250,000) by visiting the FDIC's website (www.fdic.gov), where you can search by the bank's name, city, state or ZIP code. While a bank that is not FDIC-insured may be legitimate, its customers may not be covered in case of a loss. The NCUA administers the National Credit Union Share Insurance Fund (NCUSIF), which provides deposit insurance for credit unions much like the FDIC does for banks. Visit the NCUA site (www.ncua.gov), or call, to find out if the credit union you're considering joining is insured.
- Don't spend money before it's available or your checks/payments may bounce and you may be charged an overdraft fee.
- Know how much time it takes your bank to get a payment to your creditors after receiving your online bill payment request. Some payments, typically to larger creditors, are made electronically and may reach their destination within a couple of days of your request. Payments to smaller creditors, such as your dentist, may take as long as a

week or more because the bank must write a check and mail it to the recipient. Leave plenty of time for payments to reach creditors by the due date.

- For example, what does their privacy policy say about how they'll use your personal information? Do they offer a zero-liability guarantee for any unauthorized transactions? Will they reimburse any late fees if they don't make your requested bill payment as scheduled?
- 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.
- Mobile banking activity may cost you money in higher wireless service bills. If so, consider banking online from your home computer, or inquire about other wireless service plans that better accommodate your usage.
- If you must use public Wi-Fi, take precautions. Look for the closed padlock or unbroken key in the browser frame and an "s" after "http" (in other words, "https://") in the Web address, which indicates an SSL (Secure Sockets Layer) connection. Use VPN software or a hosted VPN service to set up a "virtual private network," which provides encryption over an unencrypted Wi-Fi connection.

Vetting Financial Institutions, Online Merchants and App Providers (5 minutes)

Introduction: Using a mobile device means you may be doing everything from banking and shopping online to making instant payments or buying apps, ringtones and other products. It can become second nature to simply click a button and make a purchase or payment. But it's important to know just who you're giving your money—and your personal and account information—to and that they are trustworthy.

Ask: *What do you need to know to feel comfortable giving your business to a financial institution, merchant or software developer?* (Allow time for responses before revealing the answer on the next slide. Jot down learners' responses on your whiteboard or easel pad, if you like.)

➡SLIDE #15

Go over slide bullet points, referring to slide notes:

- A fancy website doesn't make a business legitimate or trustworthy. If you're not familiar with a company's reputation, check its authenticity, customer satisfaction rating and complaint history through an online search before you submit personal or payment information. Verify information and claims (for example, call the phone number listed).
- Make sure you will receive a receipt, and then keep it until you receive, and are satisfied with, your purchase.
- What happens if you no longer want your purchase after you receive it? Will you be allowed to get a refund? Store credit? Or are all sales final? Who pays for return shipping, if you have to mail the item back? How long will it take to process your return and issue the refund or credit? Make sure you are satisfied with the return process *before* making your purchase.
- This guarantees you won't owe anything as a result of unauthorized transactions on your account and that any money taken from your account will be replaced. Your wireless carrier and other payment processors all have policies for disputing unauthorized

charges, but not all companies offer zero liability. When you have the option, use a credit or debit card with a "zero liability" policy. Generally speaking, credit cards offer the greatest consumer protections in case your purchase is unsatisfactory or undelivered, or if you have a billing dispute with the merchant.

- A closed padlock or unbroken key in the browser frame and an "s" after "http" ("https://") in the website address indicate the site is secure and encrypted (in other words, the information being sent is encoded so that only the intended recipient can read it). Logos from companies such as VeriSign and McAfee signify that a website uses encryption or other security technology to protect your data.
- A site that automatically ends your shopping or banking session after a certain period of inactivity is an example of an extra measure of security. This prevents someone from accessing your account if you walk away from the computer without logging out or closing the browser window.
- A privacy policy, which explains how customers' personal information is collected, used and stored, should be clearly posted on the company's website. Ideally, it should state that the company won't share your information with third parties (unaffiliated individuals or organizations). At the very least, you should be able to 'opt out" of having your information shared. Logos from organizations such as TRUSTe or BBBOnline signify a trustworthy or reasonably strong privacy policy. (Click on the seal to verify it's legitimate—the address that appears should match the address of the official certifying company website.) Leave the site if you are not satisfied that your privacy will be protected. If you're downloading an app, you may be able to reset the app's privacy settings to a level you're comfortable with. Be aware that some apps can track your location. Also be aware that information gathering done directly by a third party operating on the site (such as the sponsor of a pop-up ad), or one whose site you land on by clicking a link, is subject to that company's own, possibly weaker, privacy policy.

Avoiding Scams, Fraud and Malware (10 minutes)

Introduction: Technology can be very freeing—you can do more, faster, from just about anywhere, at any time of day or night. But not everyone you might come into contact with while using you computer or wireless device is trustworthy.

➡SLIDE #16

Go over slide bullet points, referring to slide notes:

- Phishing attempts try to get you to reveal sensitive information by making you believe you are communicating with a legitimate business, such as your bank. Keep the contact number, email and short code (text) for your bank and other institutions you do business with in your address book so you'll see the name come up when you get a legitimate call, email or text message.
- Phishing emails often include a link to a spoofed, or fraudulent, website. A spoofed website is a copy of a legitimate site designed to lure you into revealing your password and other sensitive information. Rather than clicking a link in an email or text message, bookmark the company's website while on the legitimate site and use that to get there. That way you'll also avoid the possibility of mistyping the web address, or URL, and landing on a spoofed site that takes advantage of customers who misspell the institution's URL.

- If the source of an app is unknown, do an online search for reviews and user feedback to find out if others have had problems with the app or the merchant.
- If you question the authenticity of an email message, text message or phone call, don't respond. Contact the company that the message is supposedly from directly to verify the legitimacy of the communication. Remember, a legitimate business will not ask you for your Social Security number, username, password or other sensitive data via a communication you didn't initiate. If you've already responded to a "phishing" email (one that fishes for your information), immediately change the password on your account and notify the institution where you have the account.
- All major email service providers offer tools for filtering out spam and phishing messages.
- Newer Internet browsers have built-in features that, when enabled, can help protect your privacy. For example, some browsers warn you when you are about to navigate to a site that may be fraudulent. Read the user manual for your browser for more information. And update your browser software regularly to take full advantage of new privacy features as they become available.
- Use anti-spyware and antivirus software and make sure they are updated regularly to avoid malicious software that can steal your information while you're online. Enable any built-in firewall—a virtual barrier between you and the Internet—your computer or device might have.

Guarding Your Data (10 minutes)

Introduction: Your personal data—the private information that could be used to access your various accounts (not just financial, but phone, medical, and even credit reports, etc.)—are very valuable. Since a Social Security number, your mother's maiden name, or a password may be all that stands between a thief and your accounts, it's worthwhile to put some extra effort into guarding that information.

➡SLIDE #17

Go over slide bullet points, referring to slide notes:

- Passwords should be at least eight characters long and use a combination of uppercase and lowercase letters, numbers and symbols. Don't make a password out of a pet's name, birthdate, or other personal information. Strong passwords should be used for your device (to turn it on or wake it up from sleep mode) and for all your banking/financial and payment apps.
- Don't share logon info, including passwords, personal identification numbers (PINs), usernames or the answers to "password hints" with anyone—resulting transactions will be considered authorized by you—and don't leave them where someone could find them. 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 and change it immediately if you think it's been compromised.
- Log off financial and payment sites when you are done with your session or if you have to step away from the computer, and close the browser window after signing off. Clear your "cached" activity on a shared computer by clicking on the "Tools" menu (in most browsers) and selecting "Clear Recent History" or something similar. (The words may be slightly different depending on the browser you use.)

- Bluetooth is short-range wireless network technology. Headsets that don't have to be plugged into the mobile device typically use Bluetooth technology. Turn off Bluetooth whenever you are not using the device, and lock it so that it can't be opened without the password.
- Email and instant messaging aren't automatically encrypted, so don't send personal information such as credit card numbers, passwords, your birthdate or your Social Security number unless you are using a service or tool that offers the ability to encrypt the message.
- Lock your home wireless network so that strangers within range or your signal can't access your Wi-Fi (wireless Internet) connection and possibly capture the data you send and receive on an unencrypted site. Do this by creating a strong password for your router and enabling its built-in encryption tool.
- If you must use public, non-password-protected Wi-Fi, make sure you are at a secure site (https://), disable file sharing, and use a VPN (virtual private network) such as "Private WiFi" to protect your identity online.
- Also known as an Internet payment service, a digital wallet enables you to make purchases online without having to enter credit card numbers or other payment information. The purchase is charged to your pre-registered account.
- Use a firewall, which is a virtual barrier between your computer and the Internet. Your computer's operating system (OS) may have a built-in firewall; make sure it's turned on.
- Don't open anything that is not from a trusted source. Don't open files or click on links in chain letters or other unsolicited or questionable email.
- When registering for an online service or account, fill out only those fields in the registration form that are required to use the service or open an account. (These are usually marked with an asterisk (*).) If you're given the opportunity to change your privacy settings, select options that result in less of your personal information being shared, at least in the beginning. Entering online contests and filling out other optional forms increases the chances that your information will be used for marketing or other purposes, sometimes by third parties that buy the information.
- Cookies are small files stored on your computer by websites you visit. They track your activity while at the site. This information often is used to target marketing efforts, but it also is used for things like remembering items in your shopping cart and recognizing you as a repeat visitor. You can set your browser to delete cookies automatically whenever you exit, or to not accept cookies at all, but these options may restrict you from visiting certain sites or may diminish site functionality. Consider enabling or disabling cookies on a site-by-site basis. Check your browser user manual for instructions.

Activity: Mobile Banking and Payment Safety (15 minutes)

➡SLIDE #18

Have participants remove the *Mobile Banking and Payment Safety* activity from their packets.

This activity can be done individually or in small groups. Instruct participants to write the correct word or phrase to clarify each statement.

Allow 5 to 10 minutes to complete the activity.

If the activity was completed individually, invite participants to raise their hands if they would like to answer. If the activity was done in groups, rotate among them, giving a spokesperson from each group the opportunity to answer when it is that team's turn.

Refer to the answer key provided for the correct word or phrase to complete each statement.

Assistance & Resources (10 minutes)

Introduction: There are a number of resources that could be helpful to you as you start banking online or banking and making payments by mobile device.

➡SLIDE #19

The resources on this list can help you with specific issues regarding getting started, resolving a transaction dispute, or dealing with a service issue.

Go over slide bullet points, referring to slide notes:

- Whether you're already an online or mobile banking customer or just getting started, you can contact your financial institution's customer service or tech support departments directly for guidance.
- Contact the app vendor or developer or the company with which you use the app regarding any mobile payment questions or issues.
- If you're dissatisfied with a purchase, try first to resolve the issue directly with the merchant.
- If you aren't able to come to an agreement with the merchant and you want to dispute a transaction, 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.

➡SLIDE #20

If you'd like more information about Internet safety, protecting your privacy and personal information, avoiding scams, and choosing a reputable merchant or financial institution, the resources on this list can help.

- OnGuard Online: The U.S. federal government and the technology industry provide information and tips to promote online safety and security.
- PRC: 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.
- FTC: The FTC educates the public about how to protect themselves in the marketplace and takes complaints about businesses that violate consumers' rights and privacy.
- FDIC: Read the Federal Deposit Insurance Corporation's tips for safe Internet banking and find out if the bank you're considering doing business with is insured.
- NCUA: Find out if a particular credit union is insured and get fraud prevention and personal money management tips from the National Credit Union Administration.

- MS: Learn how to create strong passwords, and use a tool to check the strength of your passwords.
- Visa: Financial education at the Practical Money Skills website and advice and tips for safety and security online at the company's Security Sense website.

Questions & Answers (10 minutes)

Preparation: Review the three *Digital Dollars* brochures.

Open the floor to questions.

Wrap-up and Evaluation (5 minutes)

➡SLIDE #21

Congratulate learners on their participation in the class. Thank them for attending and ask them to fill out the evaluation form and leave it on a table or in a large envelope you provide. If you will be conducting other trainings at a specific future time, announce that now and encourage learners to attend.

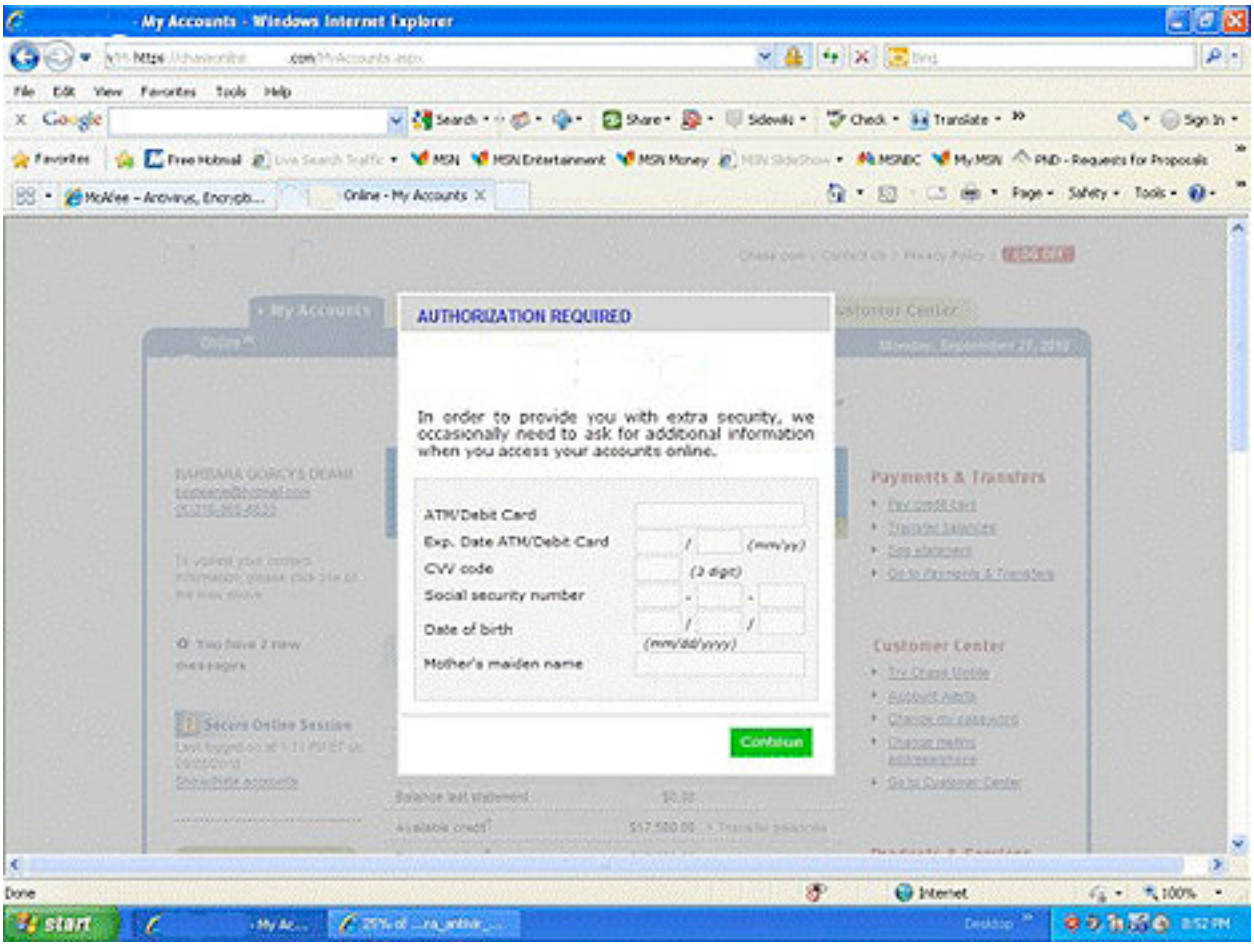
Activity: *What's 'Phish-y' About This?*

In the sample messages and websites below, circle any "red flags"—those things that might tip you off that the source is phishing for personal information. Be prepared to discuss your observations.

1) Phone call to hotel guest in room at 4:30 a.m.

"This is the front desk calling. I'm sorry to bother you but our computer system crashed and we lost all of the credit card information for our registered guests. The auditing department requires us to re-enter all our guests' payment information into the system before the start of the business day. Please give me your credit card information and we will renew your reservation."

2) Pop-up box (appears upon landing on website after clicking a link in an email message)



3) SMS text message

From: yourbank@mail.tmail.com//YourBank
debit card cancellation alert. call 212-444-4444

4) Website you land on after clicking a link in an email message

http://cgi6-secured/irsService/connection_mysql/taxaccounts.irs.com

Tax Refund Claim Form
To claim your refund, please verify your identity and mailing address below.

Name _____ _____

Address _____ Social Security # _____

Accessibility | Appeal a Tax Dispute | Careers | Freedom of Information Act | IRS Privacy Policy
©2009. IRS.gov | Internal Revenue Service | United States Department of the Treasury

5) Email message

From: no_reply@emailonline.friendly-bank.com
Subject: Account Status

Dear Friendly Bank Online[SM] Customer,

Due to recent activity on your account, we have issued the following security requirements. For your security, we have temporarily prevented access to your account. Friendly Bank safeguards your account when there is a possibility that someone other than you tried to sign on. You may be getting this message because you signed in from a different location or device. If this is the case, your access may be restored when you return to your normal sign on method. For immediate access, you are required to follow the intruction below to confirm your account in order to secure your personal account informations.

Click To Confirm Your Account

Samuel Smith
Chief Marketing Officer
Friendly Bank CardMember Services

6) Text message

recent security check requires you to re-activate your paypal account now
www.reactivatepaypal.com

7) Phone call

“I’m calling regarding your credit card. We are offering our customers the opportunity to lower their interest rate today only. Once you confirm your credit card number and expiration date, we will reduce the interest rate by 5%. You will see the reduction on your next statement.”

Key to *What's 'Phish-y' About This?* Activity

1. True story: Once the scammers figured out how to call individual rooms in a hotel, they simply dialed one after another in their search for victims. They called in the middle of the night to find more people in their rooms and to catch them while they were groggy and, perhaps, not thinking so clearly. They also knew that they would be less likely to go to the front desk to confirm the story. A hotel will *not* call a guest in the middle of the night unless it truly is an emergency. Also, major hotels are sure to have backup of all transactions on a main server, making it unnecessary to ask every guest to re-register their credit card. A guest receiving a call like this should hang up and call the front desk directly, or tell the caller that s/he will stop by the front desk with the credit card in the morning.
2. Scammers aren't just building bogus websites, they're making them fancy enough to include popup boxes that ask for your personal information. To avoid landing on a bogus website, always type in the URL (Web address) yourself rather than clicking on a link. Check that you've typed in the address correctly, since many scammers build websites with URLs that reverse a couple of letters, to take advantage of typing errors. Better yet, use a bookmark so you don't risk mistyping the address. A legitimate financial institution will never ask for this kind of personal data (Social Security number, mother's maiden name, account number, CVV security code, expiration date, and birth date) on its website.
3. This "From" address looks suspicious: An email address at mail.tmail.com does not appear to be a standard "YourBank" address despite the appearance of the name twice, once before the @ sign and once at the end. The message itself is cryptic, and there is no punctuation—misspellings, awkward language, incorrect or missing punctuation and strange formatting are all signs of fraudulent communications. The number leads to a fake call center (one scammer waiting for the phone to ring) where the "representative" will ask for your personal information, such as account number and password or Social Security number. If you get a message like this and you are concerned that it may be a legitimate alert, ignore the number, email address or link in the text message and contact the bank directly.
4. The first clue that this is not the official IRS site is that the URL doesn't begin with the real IRS homepage address (www.irs.gov). In this case, the difference is obvious, but in many cases, the scammers use a URL that closely resembles the legitimate Web address for the site they are mimicking—like www. statescredtiunion.org instead of www.statescreditunion.org, or www.charlesschwab.com instead of www.schwab.com, or www.irs.us.gov instead of www.irs.gov. Phishing attempts always ask for one or more sensitive pieces of information that a legitimate financial institution or business would never ask for online or by phone, email or text message. There is also usually a promise of money (a tax refund in this case) or a consequence (such as you account being closed) that instills urgency and requires an immediate response. Scammers copy the logos, images, fonts and formatting straight from the sites they are mimicking, so don't assume that just because the company's logo or a copyright (at the bottom of the page) appears that the site is legitimate. In this case, a consumer should either ignore the email that included the link to this site, or , if s/he were concerned about missing out on a refund, contact the IRS directly through contact information found at the real IRS site: www.irs.gov.
5. This email contains all the phishing red flags: an email address that has "friendly-bank" in it instead of the bank's true URL ("friendlybank"), a threat that account access will denied if you don't respond immediately, a link to a site that will undoubtedly request your personal data, and numerous typos ("intruction" instead of "instruction," "informations" instead of "information," US in the salutation but U.S. in the body of the email, and "CardMember" instead of "Cardmember"). And why would the Chief Marketing Officer be the one contacting

customers about their account status? Again, ignore the email entirely, or contact the bank directly to inquire about the communication.

6. Again, there is no capitalization or punctuation—unlikely in a legitimate communication from such a large company—and there is a requirement for immediate action (to avoid your account being closed). Also, the Web address appears to be bogus despite the appearance of "paypal" in the URL. In cases such as this, either ignore the text (or email) or contact the company directly using a known, legitimate phone number or Web address.
7. A legitimate financial institution will never call and ask you to provide personal data. If you're concerned you might be losing out on a great deal, hang up and call the number on the back of your card.

Additional tips:

- A link may actually appear correct (such as http://www.friendlybank.com) but be coded to lead to an entirely different URL. So always check not only that the link itself looks correct but also that the URL that appears in the browser address bar matches and is also correct.
- Any email purporting to be from a financial institution or other legitimate business that requests your personal information should be considered phony and brought to the attention of the business it claims to be from.
- While a phishing email can come from any source, statistics show that financial institutions, eBay, PayPal and the IRS are some of the identities most widely used by scammers.
- For mobile banking, get your "app" directly from the institution (available on its website) if you have the option. (There were some instances of phishing apps that temporarily appeared in at least one of the online app stores.) To avoid a mobile banking scam, it's best to disregard all messages, even if you believe them to be from your bank. Simply contact your bank as soon as possible—using a known valid email address, phone number, URL or short code—and they can tell you if any messages have been sent or if there is a problem with your account.

Activity: *Mobile Banking and Payment Safety*

Write the correct word or phrase to clarify each statement.

1. You should do this before selling, donating or disposing of your mobile device.

2. It is safest to use one of these when shopping online.

3. Set your mobile device to do this automatically when it's not being used.

4. Delete old ones of these so that they are not accessible if your phone is lost or stolen.

5. Make sure the financial institution offers this, which guarantees you won't be responsible for unauthorized transactions.

6. A strong one of these protects your personal information from being shared with third parties.

7. Using one of these allows you to avoid entering your credit card information every time you make a payment using your mobile device.

8. It's important to do this when you're finished using a financial app.

9. This type of Wi-Fi can leave your information vulnerable when shopping or banking by mobile device or computer.

10. If you receive a text or email message from your financial institution asking for your password, PIN, Social Security number or other sensitive information, it's best to do this.

11. These types of communication are not typically encrypted, so it's best not to send sensitive information using them.

12. Special software can help you do this if your phone is lost or stolen.

13. A strong password should be this long.

14. Before downloading an app from an unknown source, do this.

15. Add your bank's short code to your phone's contact list to know if one of these is actually from your bank and not a scammer.

16. Do this to avoid landing on a fraudulent site because you mistyped the bank's Web address.

Key to *Mobile Banking and Payment Safety* Activity

1. You should "*erase your hard drive completely and permanently"* before selling, donating or disposing of your mobile device. (erase your hard drive completely and permanently)

2. It is safest to use "*a credit card*" when shopping online. (a credit card)

3. Set your mobile device to "*lock*" automatically when it's not being used. (lock)

4. Delete old "*transaction text and email messages*" so that they are not accessible if your phone is lost or stolen. (transaction text and email messages)

5. Make sure the financial institution offers "*a zero-liability policy,*" which guarantees you won't be responsible for unauthorized transactions. (a zero-liability policy)

6. A strong "*privacy policy*" protects your personal information from being shared with third parties. (privacy policy)

7. Using "*a digital wallet or Internet payment service*" allows you to avoid entering your credit card information every time you make a payment using your mobile device. (a digital wallet or Internet payment service)

8. It's important to "*log out and close the app*" when you're finished using a financial app. (log out and close the app)

9. "*Public, non-password-protected*" Wi-Fi can leave your information vulnerable when shopping or banking by mobile device or computer. (public, non-password-protected)

10. If you receive a text or email message from your financial institution asking for your password, PIN, Social Security number or other sensitive information, it's best to "*ignore or delete it and contact the institution directly.*" (ignore or delete it and contact the institution directly)

11. "*Email and instant messaging (IM)*" are not typically encrypted, so it's best not to send sensitive information using them. (email and instant messaging/IM)

12. Special software can help you "*locate the device or remotely "wipe" the data*" if your phone is lost or stolen. (locate the device or remotely "wipe" the data)

13. A strong password should be "*at least eight characters, combining uppercase and lowercase letters, numbers and symbols*." (at least eight characters, combining uppercase and lowercase letters, numbers and symbols)

14. Before downloading an app from an unknown source, "*search online for reviews and user feedback*." (search online for reviews and user feedback)

15. Add your bank's short code to your phone's contact list to know if "a text, or SMS, message" is actually from your bank and not a scammer. (a text, or SMS, message)

16. "*Bookmark your bank's website*" to avoid landing on a fraudulent site because you mistyped the bank's Web address. (bookmark your bank's website)

Training Evaluation: *Your Digital Dollars*

Date and Location of Training:_____

Please help us improve future presentations by giving us your opinion of today's class. Circle the response that best reflects your feelings about each statement:

1. I have a better understanding of how online and mobile banking and payments work.

Strongly agree Agree Disagree Strongly disagree

2. I understand the benefits and risks associated with digital transactions.

Strongly agree Agree Disagree Strongly disagree

3. I know what steps to take and what tools to use to protect my personal information, device, data and accounts and to make every transaction more secure.

Strongly agree Agree Disagree Strongly disagree

4. I know where to go for more information and assistance on this subject.

Strongly agree Agree Disagree Strongly disagree

5. I can use what I learned today to make improvements in my life.

Strongly agree Agree Disagree Strongly disagree

6. The instructor was well informed.

Strongly agree Agree Disagree Strongly disagree

7. The materials I received are easy to read and understand.

Strongly agree Agree Disagree Strongly disagree

8. I would like to attend another class like this.

Strongly agree Agree Disagree Strongly disagree

Please let us know how we could improve future trainings (use back, if necessary):

_____

_____

_____

_____

_____

Thank you for attending!