Put a Lock on It

Protecting your online privacy

Seminar lesson plan and activities

www.consumer-action.org

Through multilingual consumer education materials, community outreach and issue-focused advocacy, Consumer Action empowers underrepresented consumers nationwide to assert their consumer rights and prosper.

Consumer advice and assistance: Submit consumer complaints to our advice and referral hotline: www.consumer-action.org/hotline/complaint_form or 415-777-9635.

Chinese, English and Spanish spoken

This publication was created in partnership with Google.

© Consumer Action 2015
Lesson purpose:
To provide participants with an understanding of the potential privacy risks for Internet and mobile technology users and the many effective tools and practices available to them to achieve the level of privacy and data security that they desire for themselves and their family.

Learning objectives:
By the end of the lesson, participants will understand:
• why it's important to play an active role in protecting their online and mobile privacy;
• what privacy tools and account settings may be at their disposal;
• non-technical ways to stay safe when shopping or banking online or by mobile device;
• how to download and use apps safely;
• how to avoid scams and malware;
• how data breaches happen and what they can do if they are part of one;
• the potential risks of “oversharing” on social media and how to avoid unwanted exposure;
• what parents can do to make the Internet and mobile apps more family friendly;
• how to exercise some control over who collects their personal data and how they use it; and
• where to find more information about online and mobile privacy and safety.

Lesson duration:
2½ hours

Materials:
For instructor:
• Put a Lock on It: Protecting your online privacy (brochure)
• Visual teaching aid (PowerPoint presentation with instructor’s notes)
• Lesson plan, including activities and answer keys (pages 3-30)
• Class evaluation form (page 31)

Instructor will also need:
• a computer and projector for the PowerPoint presentation (the PowerPoint slides also can be printed on transparency sheets for use with an overhead projector); and
• an easel and pad, or a whiteboard, and markers.

For participants:
• Put a Lock on It: Protecting your online privacy (brochure)
• “Are you cyber savvy?” activity (1 page)
• “Something’s phish-y” activity (4 pages)
• “To share or not to share?” activity (2 pages)
• Class evaluation form (1 page)

Optional:
• Printout of the PowerPoint presentation
Lesson outline (and suggested times):

- Welcome and training overview (5 minutes)
- Locking your accounts (15 min)
- Secure transactions (includes activity) (25 min)
- Mobile device safety (10 min)
- App safety (10 min)
- Avoidable threats (includes activity) (20 min)
- Data breaches (5 min)
- Social media privacy (includes activity) (25 min)
- Family-friendly Internet (10 min)
- Online marketing and data collection (10 min)
- Resources (5 min)
- Questions and answers (5 min)
- Wrap-up and evaluation (5 min)
Instructor’s notes:

This training module consists of a fact sheet/brochure (*Put a Lock on It: Protecting your online privacy*), a lesson plan with class activities, and a PowerPoint presentation. It was created by the national non-profit organization Consumer Action to be used by non-profit organizations providing consumer education in their communities.

Before conducting the training, familiarize yourself with the fact sheet, 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). These notes offer detailed information about the items appearing on the slide. The learning objectives for each section, along with key points and questions to generate discussion, are included in the lesson plan, as are indicators telling you when to move to the next PowerPoint slide.

*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 [www.consumer-action.org/outreach/articles/why_adults_learn/](http://www.consumer-action.org/outreach/articles/why_adults_learn/).

---

**WELCOME AND TRAINING OVERVIEW** (5 minutes)

➡️ **SLIDE #1** (onscreen as participants arrive; direct early arrivals to begin reading the fact sheet)

**Welcome** participants and introduce yourself.

If you have a small group, you can ask individuals to introduce themselves (or, if time permits, ask them to pair off with someone seated near them and then introduce each other to the group) and tell you what they hope to get out of the training. In a larger group, invite a few 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 class 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.)

**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.

➡️ **SLIDE #2**

**Present** what participants will learn during this seminar.

**What you will learn**

- Why it’s important to play an active role in protecting your privacy online
- What tech tools are available to you
- How to avoid oversharing on social media
- Ways to keep kids safe on the Web and mobile devices

**Slide notes:** People of all ages and backgrounds use computers and Internet-enabled devices to work, learn, play games, listen to music, watch videos, stay in touch with friends and family or just “surf the Web.” Being “connected” has become such a part of daily life for most people that it’s easy to forget the potential risks associated with the enjoyment and convenience. Over the next couple of hours, you will learn about specific ways to protect yourself and your family from potential risks—identity or data theft, for example—while still taking advantage of everything the Internet and mobile technology have to offer.

**• Playing an active role:** Online privacy and security is a shared responsibility: Companies need to employ privacy “best practices” and implement the latest privacy and
security technology, and consumers need to stay aware of changes in privacy protections and risks, keep their operating systems and software updated, and use the privacy tools and account settings at their disposal. By being an active participant, you can achieve the desired level of privacy and the greatest level of personal data protection possible.

- **Tech privacy/security tools:** Many tools exist for keeping intruders out of your financial, email and social media accounts, computer and mobile devices, etc. Once you know what they are, you can make sure to look for them on the sites, apps and devices you use.

- **Safe social media sharing:** Sharing is good—oversharing, or sharing with the wrong people, is risky. Tips and tools will help you share only what you want, with the audience you choose.

- **Family-friendly Internet and apps:** You can’t keep kids from getting online, but you can make the Internet and mobile apps more family-friendly by implementing parental controls and helping your children make wise choices.

**LOCKING YOUR ACCOUNTS (15 min)**

**Learning objective:** Understand how passwords help to protect your accounts and the importance of using the strongest security tools at your disposal.

**Key points (slides 3-5):**
- The best way to avoid having your privacy violated or your personal data stolen is to keep intruders out of your accounts from the start.
- A strong password is the first line of defense against hackers and others.
- Two-factor authentication is even stronger than a password alone, and should be enabled wherever it’s available.

**Questions to generate discussion:**
- Has anyone ever guessed, or hacked, your account password? Why/how do you think that happened? Could you have prevented it?

*Note: When generating discussion, allow a moment or two for participants to respond. You can jot down responses on your easel pad or whiteboard.*

➡ **SLIDE #3**

**Introduction:** Passwords have been used for centuries to keep unwanted visitors out—that says a lot about their effectiveness! The ways we create, manage and store passwords may be very different in the digital age than they were many years ago, but passwords still play an important role in keeping our confidential information out of reach of others.

**Go over slide notes.**

**Slide notes:** The “password” is the most basic and widely used method of securing an account. Its effectiveness depends on the strength of the password you create, your commitment to keeping it secret and your diligence in changing your password as needed.

- Create a password that is at least eight characters long and a random mix of upper and lowercase letters, numbers and symbols (if the site/app allows the use of symbols). The longer the password is, the harder it is for an intruder to crack—some experts now recommend passwords that are at least 10 characters long. Avoid using actual
words (anything found in the dictionary) or personal information such as your birth date or pet’s name. Don’t use the same password for all your accounts. Having different passwords ensures that someone who gets your password for one account won’t be able to get into all your accounts.

• Rather than writing them down, use a tool that stores all your passwords and requires you to remember only one. You can learn about password managers from PCMag.com (www.pcmag.com/article2/0,2817,2407168,00.asp) and Lifehacker (http://lifehacker.com/5529133/five-best-password-managers). Some free options are LastPass, KeePass, 1Password, Dashlane and RoboForm. (Creating a password out of the first letters of a sentence or phrase can help you remember it—for example, you could create the password Ih2D&1C! out of the sentence “I have two dogs and one cat!”)

• If you are asked to select security questions that will allow you to get into your account if you forget your password or are on an unrecognized computer or device, choose ones that it would be difficult or impossible for someone else to know or guess the answer to (for example, “Who was your first kiss?” or “Who was your third grade teacher?” is probably more difficult to look up than “What is your mother’s maiden name?”).

• Log out of your account when you are finished and, if you share a device with others, don’t let your browser save your login information (i.e., don’t click the “Remember me” box, as seen in slide image). Click the “Not now,” “Never for this site” or similar option when prompted to allow the browser to save your password, or check/uncheck the appropriate boxes in the Security, Passwords, Sync or AutoFill tabs of the browser’s Settings or Preferences. Likewise, don’t let online retailers save your credit or debit card information.

• Require a login password to start up your computer or to “wake” it. That adds another layer of protection against anyone who tries to get into your accounts from your own computer. Learn how to do this for an Apple (Mac) (www.apple.com/support/osx/passwords/) and a PC (http://pcsupport.about.com/od/tipstricks/ht/newxppassword.htm).

➡ SLIDE #4

Ask participants to assess the strength and weakness of the passwords on the slide.

<table>
<thead>
<tr>
<th>Strong or weak?</th>
<th>Slide notes/answers: Which of these passwords are strong and which are weak. Why? Which is the strongest?</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEO123</td>
<td>password</td>
</tr>
<tr>
<td>12345</td>
<td>amazon1</td>
</tr>
<tr>
<td>Abc123</td>
<td>6&amp;rT&amp;4Hd</td>
</tr>
<tr>
<td>FT2rY&amp;s1L</td>
<td>n3k6c2s</td>
</tr>
</tbody>
</table>

and is, in fact, the most commonly used password. amazon1 is weak because it is only seven characters long, contains mostly lowercase letters, and could be very easy for someone to guess—particularly if it is being used as the password for the user’s Amazon account. n3k6c2s is not that far off from being a strong password—it contains a seemingly random series of letters and numbers—but it is only seven characters long and does not contain any uppercase letters or symbols.

• The strongest password on this list is FT2rY&s1L. It is even better than the next best one—6&rT&4Hd—because it contains one extra character (nine instead of eight).

Go over slide notes.

---

**Two-factor authentication**

Slide notes: Two-factor authentication is much stronger protection than a password alone. It requires a second level of authentication to access the account—for example, a password and confirmation of an onscreen picture/graphics you’ve chosen, or a password and a fingerprint scan, or a password plus a passcode that is sent to you via text message or email. It’s like having to swipe your debit card and enter a PIN at the grocery store or swiping your credit card and entering your ZIP code at the gas station.

- Enable two-factor authentication wherever it’s an option. Not all sites offer it, but many do, including Google, Apple, Facebook, Twitter and PayPal, just to name a few. Each site has its own instructions for enabling 2FA. Check “Settings,” first. If you can’t find it there, contact the website’s Support team.

- Learn more about two-factor authentication from Stop.Think.Connect. ([http://stopthinkconnect.org/campaigns/details/?id=460](http://stopthinkconnect.org/campaigns/details/?id=460)). This list displays many sites that offer 2FA and many that don’t: [https://twofactorauth.org/](https://twofactorauth.org/). This site provides step-by-step instructions on how to enable 2FA on many of the most popular sites: [https://www.turnon2fa.com/](https://www.turnon2fa.com/).

---

**SECURE TRANSACTIONS** *(25 min)*

**Learning objective:** Understand both the technical and non-technical ways to stay safe when shopping or banking online or via mobile app.

**Key points (slides 6-8):**

- Financial institutions dedicate significant resources toward maintaining a secure online and mobile banking system. Because of this, online and mobile banking may be safer than you think.

- You can achieve some degree of account and data security just by being careful, exercising common sense and trusting your instincts.

- Encryption (data scrambling) and a firewall (a software-created barrier between your computer and the Internet) are important tools in preventing hackers from tracking your online activity or stealing your sensitive information.

**Questions to generate discussion:**

- Do you shop or bank online or using a mobile app? Why or why not? If not, what would make you decide to start?

- Why do you think financial institutions and large retailers put resources toward protecting their customers’ data? *(It saves them money in the long run and helps them keep their customers; in the case of banks, it puts them in compliance with federal regulations governing customer account safety.)*

- What are three things you could do to make your online or mobile banking activity safer and more secure?
**Introduction:** Banking conducted via computer or mobile device offers many advantages over branch banking, including being able to receive text and email alerts about your account, check your account balance and transactions in real time, pay bills and transfer funds without ever leaving your home or office, and make a deposit in a snap just by taking a photo of the check—at any time, from anywhere. Likewise, shopping online or via a mobile app can save you time, make it easier to comparison shop, allow you to save items in your “shopping cart” for a future purchase, entitle you to coupons and insider sales and allow you to read customer reviews of products you’re considering. Financial institutions and retailers generally make it their priority to ensure a safe, problem-free banking or shopping experience, but there are things you can do yourself to further safeguard your personal data.

**Go over slide notes.**

**Secure transactions**

- Mobile banking
- Online shopping

**Slide notes:** Millions of consumers shop and bank online because doing so saves them time and money. Since there are many ways—technical and non-technical—to keep your accounts and data safe, there’s really no reason to forego online and mobile transactions as long as you take precautions. What are some of the non-technical ways to stay safe when shopping or banking via computer or mobile device?

- Try to shop only with online merchants you know and trust.
- Vet online merchants you are unfamiliar with. Check reviews and complaints, if any. Check them out with the Better Business Bureau (www.bbb.org).
- Trust your instincts—use good judgment when evaluating an online merchant, email solicitation, marketing post, etc. If something appears too good to be true, it probably is.
- Use a credit card rather than a debit card. If something does go wrong, a credit card offers greater protection against fraudulent transactions: $50 maximum consumer liability (oftentimes $0) and the right to dispute charges and withhold payment during the investigation. (Liability for unauthorized use of a debit card can be much higher, depending upon when you report the loss. And most debit cards are linked to your bank account, which means a thief could wipe you out.)
- If you are shopping or banking by mobile phone, be sure that no one can overhear you providing your bank account or credit/debit card number.

**Encryption**

**Slide notes:** Encryption is a technology that scrambles (encrypts) the electronic information being sent through cyberspace so that it is much more difficult for hackers to track your activity or steal your data. There is website encryption and network encryption—having both is most secure.

- To determine if a website uses encryption, look for the “s”, which stands for “secure,” in the URL (https:// rather than just http://). You might also see a padlock, or the address bar itself might turn green when you enter a secure website. (See slide image for an example off all three indications of encryption: https, padlock and green address bar.) Look for one or more of these assurances before you make a purchase, access your financial accounts or conduct any type of transaction.
• Some standard email and text messages are not encrypted, so never send account numbers, your Social Security number or other sensitive information this way.

• If you have Wi-Fi at home, you have a wireless router—make sure the router’s encryption feature is turned on (they often come with it turned off). At the same time, create a strong network password (at least 14 characters) for your router to prevent intruders in range of your Wi-Fi signal from accessing your connection. Get details about securing your wireless network from OnGuardOnline.gov (www.onguardonline.gov/articles/0013-securing-your-wireless-network).

• Because you can’t always be sure that an outside network is encrypted, use your wireless carrier’s network rather than public Wi-Fi for shopping or banking when you’re away from home. Consider changing the settings on your mobile device so that it doesn’t automatically connect to nearby Wi-Fi—that way you can make a case-by-case decision depending on what you plan to do online. Learn more about using public Wi-Fi safely from OnGuardOnline.gov (www.onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks).

• Regularly clear the browser history to prevent anyone who finds or steals your phone from retracing your steps to hijack your accounts.

➡ SLIDE #8

Go over slide notes.

Slide notes: Most computer operating systems come with a built-in firewall—a barrier between the outside world and your computer.

• Firewalls typically are activated by default by the manufacturer on newer computers, but they may not be activated on older machines. As a result, older computers with “always on” high-speed Internet connections may be at risk for security and privacy breaches. To be safe, check your computer’s Security settings (often found under “Preferences”) to make sure your firewall is on. If you are having trouble finding the controls, do an online search for the word “firewall” along with the name of your computer operating system to get instructions.

• Download antivirus and firewall software that’s made for your operating system if it’s not already installed, and keep it up to date. Ratings sites such as TopTenReviews.com (http://anti-virus-software-review.toptenreviews.com) and online magazines such as PCMag.com (www.pcmag.com/article2/0,2817,2372364,00.asp) can help.

Assign the “Are you cyber savvy?” exercise (page 20). Have participants complete the exercise individually or in small groups. Do not advance to the next slide until participants are finished with the exercise. Answer key is on pages 21 and 22.

MOBILE DEVICE SAFETY (10 min)

Learning objective: Understand the unique security risks that mobile devices pose and be aware of the precautions you can take to protect your devices and your data.

Key points (slide 9):

• A mobile device that you use for banking, shopping and other transactions can be just like a wallet, and should be watched with the same care.

• Because mobile devices go with you, they are at higher risk to be lost or stolen than a full-size computer, which means you have to take extra precautions to protect them and the data they hold.

• The single best thing you can do to protect your data is set your device to lock after a few minutes of inactivity and require a PIN/passcode (or thumbprint) to unlock.
• It’s smart to use a locate/lock/erase app so that you can track a misplaced or stolen device, lock it until you get it back, or erase the data if you believe it’s fallen into the wrong hands.

Questions to generate discussion:
• What kind of information do you think a thief could get from your smartphone? How do you think s/he could use that data?
• Is your smartphone or tablet set to lock and require a PIN/passcode/thumbprint? If not, why not?

Introduction: The benefit of a smartphone or tablet is that you can take it with you and be able to do most of the same things you could do on a full-size computer, anywhere you go. That provides a lot of convenience—and some risk. But you can greatly reduce the chances of your personal accounts being accessed or your sensitive data being stolen by taking a few precautions.

Go over slide notes.

Slide notes:
Because of their size and portability, phones and other mobile devices are at greater risk than computers of being lost or stolen, which means you have to take additional or different precautions to protect them and the data they contain.
• Keep an eye on your mobile device just as you would your wallet—a smartphone containing financial account information, financial and shopping apps and personal identification information is just as valuable to some thieves.
• Start by locking your device with a PIN/password (or thumbprint, depending on the version). Set it to lock after a few minutes of inactivity. Also turn off Bluetooth when you don’t need it; disabling the Bluetooth service will decrease a hacker’s ability to wirelessly hack into your phone.
• Use a remote locate/lock/erase app such as Find My iPhone (Apple) or Android Device Manager. This allows you to find your device if you’ve misplaced it, or remotely lock it or delete your data if it’s lost or stolen.
• “Wipe” the data off your device before you sell, donate or dispose of it so nobody else can access your personal information. CTIA-The Wireless Association offers tips and links to instructions for erasing the information on your particular type of mobile device (www.ctia.org/your-wireless-life/consumer-tips/tips/how-to-erase-data-on-your-mobile-device). Money Talks News offers instructions for wiping smartphones, tablets and laptops (www.moneytalksnews.com/how-make-sure-your-data-wiped-from-old-electronics/).
• Learn more about cyberproofing your phone from AARP (www.aarp.org/home-family/personal-technology/info-2014/cyberproof-stolen-phone-kirchheimer.html).

OPTIONAL: If there is time and you think it would be beneficial to participants, allow a few minutes for anyone who hasn’t set their smartphone to lock to do so now. (Apple/iOS instructions: https://support.apple.com/en-us/HT204060; Android instructions: https://support.google.com/nexus/answer/2819522?hl=en; and Windows Phone instructions: www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/lock-screen-faq).

APP SAFETY (10 min)

Learning objective: Understand how to choose and use apps wisely to avoid compromising your privacy or putting yourself or your data at risk.
Key points (slide 10):

• It's possible to avoid risky apps—those that use your data in ways you don't want, invade your privacy or install malware—if you are careful about how you choose and use apps.

• You should use the app’s settings to control what information it collects and shares. If you don’t like its data use practices or privacy policy, don’t download it—choose a different app.

• To protect your personal safety and privacy, don’t allow apps to announce your location to strangers. (Some apps, such as those that provide maps and directions, use your location to provide a service but don’t make it public.)

• You should set your apps for automatic updates so that you ensure you have the newest—and, most likely, safest—version available.

• You can uninstall an app if you don’t agree with changes it makes in its data use or privacy policies.

Questions to generate discussion:

• How many apps do you think you have on your smartphone or tablet right now? How many of those apps’ data use and privacy policies have you read? If none, why not?

• Can you think of any reasons why allowing an app to share your location with others (such as posting on Facebook that you just “checked in” at the gym) could be risky? What could someone do with that information?

➡SLIDE #10

Introduction: Apps—software applications designed specifically for mobile devices—are powerful tools. They make it possible to do everything from request a ride and order a meal to deposit a check and track how many steps you've taken today. Such powerful tools are great if they work for you, not against you. You can make sure that all your apps are trustworthy by taking a few precautions.

Go over slide notes.

Slide notes:

“Apps” are software applications designed specifically for mobile devices. Apps put the functionality into your device, allowing you to stream music, check the weather, play a game, deposit a check, track your exercise, etc. If you want to get the most out of your device, you need apps, but there are some safety precautions to take before and after downloading an app.

• Vet your apps. Only download apps from trusted sources. Read user reviews and make sure the developer is legitimate before downloading. Download the mobile banking app you need directly from the financial institution’s website. When using your smartphone to shop, use retailers’ apps rather than your phone’s browser. (Because they don’t use Web browsers, apps are resistant to phishing scams (for example, you can’t mistype the URL and end up on a spoofed site). However, to preserve your security, you must log out of the app when you are finished, and disable any function that saves your login information.)

• Set your apps for the desired level of privacy. Many apps depend on the ability to retrieve and share users’ personal information, such as contacts, calendars and even location. To control what an app collects and shares, check the settings in the app itself (as opposed to the device settings). If the app wants to collect more personal data then you are comfortable with, don’t download it. Review the app’s privacy policy, if it has one. If it doesn’t, consider choosing a different app.
• **Avoid apps that announce your location**, or disable that function if you have the option. Sharing your physical location with others could put you at risk of a home robbery or otherwise compromise your safety and privacy. (Some apps, such as those that provide maps and directions, use your location to perform a function but don’t make it public.)

• **Opt for automatic updates** of your operating system and apps or install software updates as they become available to ensure you always have the newest version of the app available. (Updates often improve safety by addressing a known security issue.)

• **Read notifications of changes** to the app’s terms of use or privacy policy so that you can uninstall the app if it plans to collect or share more of your data than you want. Depending on the app and the significance of the changes, you may receive a direct notification (typically by email or from within the app, know as a “push notification”). In other cases, the only way you’ll find out about a change might be to revisit these sections in the app or at its website.

---

**AVOIDABLE THREATS** *(20 min)*

**Learning objective:** Understand how to spot and avoid dubious messages and malicious software and sites.

**Key points (slide 11):**

- Most “phishing” emails contain tip-offs that they are bogus. Look for sloppy grammar, unnecessary capitalization, misspellings, unprofessional or strange wording, requests for private info, and attempts to create urgency.
- A legitimate business or government agency will never ask you to provide things like your password, Social Security number or bank/credit card number via email.
- If you are suspicious of a communication or website, you should trust your gut.
- You should never respond to spam, phishing emails or any other dubious communication—ignore and delete.
- Malware and spyware often comes from downloaded apps and files or opened links. Only download apps and files from trusted sources, and don’t click on links sent to you by anyone you don’t know.

**Questions to generate discussion:**

- Why do you think “phishing” emails are so named? *(Because the sender is “fishing” for your information. The use of “ph” instead of “f” comes from “phreaks,” the name given to some early hackers.)*
- Why do you think scammers put so much effort into creating phishing emails and spoofed websites? *(Because despite consumer education efforts, they still get many victims to “bite.”)*

➡ **SLIDE #11**

**Introduction:** Schemes designed to get your personal information have been around for ages. While you can’t stop scammers from scamming, you can thwart their efforts by staying on guard and being smarter than they are. The schemes may change, but general rules of thumb still apply—know who you can trust; if it sounds to good to be true, it is; and, it’s better to be proactive than reactive.

Go over slide notes.
Whether you’re using a computer or a mobile device, some risks are almost entirely avoidable if you know what to look for and you stay on guard.

Phishing is an attempt to "hook" you into revealing confidential information by sending bogus emails that appear to come from a financial institution, company, retailer, social networking site or government agency. The messages use the company’s or agency’s same colors, logos, fonts and layout (spoofing) and often include a link to a legitimate-looking but phony web page where you are asked to enter your personal information. Tip-offs that an email may be phishing are bad grammar, incorrect punctuation, misspellings and awkward language; the use of phrases such as “Verify your account” and “Your account will be closed”; and a request for your login information, credit card number, etc. A legitimate business will never ask for personal information via email. Verify the email directly with the company or agency—but not by using contact information provided in the e-mail. Do not reply to the email. Forward phishing emails to spam@uce.gov and to the company, bank or organization being impersonated. Learn more from the FTC (www.consumer.ftc.gov/articles/0003-phishing). Many web browsers block spoofed websites or alert users who try to visit a fraudulent site or download malicious software—another reason to keep your browser software up to date.

Spam is unwelcome email, text and instant messages, which may offer questionable goods for sale or a promise of financial reward if you give the sender money. Ignore and delete spam completely. Do not open or respond, even to unsubscribe. Most Internet service providers (ISPs) and email programs now include an automatic spam filter—manage the filter in your email settings.

Malware is malicious software that can be remotely installed on your computer or mobile device, allowing the person who controls the malicious software to damage or delete your files and/or steal data (typically login IDs, passwords, account information and credit/debit card numbers). Similarly, spyware allows the perpetrator to track your online activity. Often, the malware or spyware is embedded in an app you download, an email attachment you open or a file you get from the Internet. Don’t open files and messages from individuals you do not know. Get your apps only from well-known app stores or the official websites of the companies you do business with. Install antivirus and antispyware software on your computer and set it to update automatically.

Malicious websites are harmful sites that lure users by promising content on popular breaking news stories, offers from retailers or other desired information. Links to such sites can appear among online search results, be sent to you via email or show up on social media. Never open links that are sent to you by anyone you don’t know. When doing an online search, visit only well known, trusted sources of information.

Assign the “Something’s phish-y” exercise (four pages beginning on page 23). Have participants work on it individually or in small groups. Or display each of the four exercise images onscreen (copy and paste one image into each of four new slides you insert into the deck) and allow the class to do the exercise together. Answer key is on page 27.

DATA BREACHES (5 min)

Learning objective: Understand what a data breach is, the limited opportunity you have to avoid becoming a victim and what to do if you do.

Key points (slide 12):

- A data breach does not mean that you will definitely become an identity theft victim, though that is a possibility.
• There is not much you can do to prevent a data breach because you are not in control of the databases containing your information, but you may be able to reduce the odds of becoming a victim by being selective about whom you share your sensitive data with.

• A security (or “credit”) freeze is an option for consumers who are at significant risk of identity theft, though it won’t prevent thieves from accessing existing accounts.

Questions to generate discussion:
• Do you worry that you will be part of a data breach? Why or why not?
• Is there anything you do now that you believe helps you avoid becoming a data breach victim? If so, what?

➡ SLIDE #12

Introduction: Data breaches—the unauthorized or illegal viewing, access to or retrieval of sensitive information—have, unfortunately, become a fact of life. That doesn’t mean that you are destined to become a victim of identity theft. But it does mean you should limit the sharing of your personal data as much as possible, pay attention to anything you receive notifying you that your data has been breached and take steps to limit the repercussions.

Go over slide notes.

Slide notes: What’s a data breach? A data breach is an incident that involves the unauthorized or illegal viewing, access to or retrieval of sensitive information. A data breach can occur accidentally (for example, if an employee loses a laptop) or intentionally (if a hacker targets a database). A breach does not necessarily mean you will be the victim of identity theft, though that is a possible result. It depends on the type of data breached (for example, a list of just names versus a list of Social Security (SSN) numbers), who obtained the information and what their intentions are.

How can you avoid one? There’s not much you can do to prevent a data breach since you are not in control of the databases containing your information. However, you might be able to reduce the odds of being affected by a breach by being selective about who you give your sensitive data to—the fewer third parties that have your information, the fewer opportunities there are for you to be included in a breach. Also, whenever possible, limit the amount of your information companies and service providers keep on file. For example, don’t allow websites to keep your credit card information on file and resist giving your SSN to health care providers (despite there being little, if any, reason for them to have it, some refuse service if you won’t provide it).

What can you do if you’re a victim? What you do will depend on what information was breached. If it was highly sensitive, such as your SSN or financial account numbers, consider placing a security (or “credit”) freeze on your credit reports. This restricts access to your credit report, which makes it virtually impossible for someone to open new accounts in your name. (If a prospective creditor can’t see your file, they most likely will not extend credit.) To place a freeze, contact each of the nationwide credit reporting agencies: Equifax, Experian and TransUnion. A security freeze doesn’t prevent a thief from making charges to your existing accounts, so you’ll still need to monitor all bank, credit card and insurance statements for fraudulent transactions. If the company that experienced the breach is offering free identity theft monitoring services to victims, sign up (though the effectiveness of such monitoring services is limited). Change the passwords on your other accounts to prevent thieves from accessing those. Learn more about placing a security freeze (www.consumer.ftc.gov/articles/0497-credit-freeze-faqs) and what to do if you become a victim of identity theft (www.consumer.ftc.gov/features/feature-0014-identity-theft) from the FTC.
SOCIAL MEDIA PRIVACY (25 min)

Learning objective: Understand the risks of oversharing on social media and how to manage your social media activity and account settings so that you achieve the level of privacy you desire.

Key points (slides 13-14):
• Wise social media use means always asking yourself how much you should share and with whom.
• Social media accounts come with settings that you can adjust to match your privacy goals. However, anything you intentionally share with a limited audience can be re-shared by them with a much wider and unintended audience.
• Generally speaking, apps have the potential to access most of the information in your phone, including your contacts, your emails and texts and your location, so it’s particularly important to pay attention to app policies and settings.
• Your e-reputation is worth managing and protecting since it can weigh heavily in people’s impression of you—particularly, if they don’t know you personally.

Questions to generate discussion:
• What are some examples of “oversharing”? What are some potential repercussions of oversharing?
• Thinking about your social media activity (posts, tweets, photos, videos, etc.), what assumptions might someone who doesn’t know you personally make about you? Would their assumptions be correct? Do you think you have a positive or negative online reputation?
• Have you ever “Googled” your name to see what pops up in the search results? If yes, were you surprised by anything?

➡ SLIDE #13

Introduction: Using social media to create or join a community can be very rewarding. But if you don’t consciously manage your participation, it can also expose you to unintended audiences and potentially significant consequences. Protecting your privacy and reputation requires smart choices about what to share and with whom.

Go over slide notes.

Slide notes: Social media is such an integral part of everyday life for many people that it can be easy to forget that it’s not just you chatting around the table with a close group of friends. To avoid the potential consequences of oversharing, think about how the information you reveal could be used, and use the tools available to control what others see.

• Adjust the social media network’s privacy settings to match your comfort level—from not sharing with anyone to sharing with the general public. The default settings are not the same for each social network, and on some networks they may be set for less privacy than you would like. First, log in to your account, then look for a tab or heading such as “Privacy,” “Privacy Controls,” “Privacy Settings,” “Account Settings” or “Preferences.” If you’re having trouble finding it, use the site’s “Help” feature, or email the website’s Support team. Options on a few popular social networks include: “Change your profile photo & visibility,” “Select who can send you invitations” and “Protect my Tweets.” You may be able to access controls when you share so that you can
specify a different audience for each individual communication. Even if you fail to make a choice before sharing, you should be able to change the audience setting by “editing” existing posts.

• Generally speaking, apps can access most of the information in your phone, including your list of contacts and your emails and texts, without your direct permission, but some apps will ask for your consent to access more sensitive information such as your location. To manage the settings for social media apps, look for “Apps,” “Data Sharing” or a similar term in the social media site’s Help menu, Preferences or Settings.

• Don’t share personal information—your full name, address, phone number, mother’s maiden name or year of birth, for example—that routinely is used for identification purposes. And don’t share current location and travel plans, which could put you or your property at risk.

• It’s a good policy not to accept invitations or “friend” requests from people you don’t know.

• Learn more in Consumer Action’s publication Privacy and Control for Social Media Users (www.consumer-action.org/english/articles/privacy_and_control_for_social_media_users).

➡ SLIDE #14

Go over slide notes.

Protecting your online reputation

Slide notes: Managing and protecting your digital reputation can save you from embarrassment and allow you to avoid the potential consequences of not putting your best foot forward.

• Consider what an employer, recruiter, college admissions officer, lender, landlord, customer/client, government agency, insurer or other decision maker would think about what you’re sharing. Realize that many people you do not know personally may turn to social media to learn something about you.

• Be aware that a “friend” can repost, retweet or otherwise expose what you assumed you shared only with your selected audience. And if you post something to another person’s profile, you have no control over who else sees it.

• Backtrack if necessary. Some social media sites enable you to delete posts, remove photos, change audiences, etc. so that things you shared in the past aren’t visible to future viewers. (Of course, you can’t do anything about everyone who has already seen what you’ve shared.)

• “Google” your name to see what pops up. Ask others to remove unflattering photos, videos or posts that include you.

• Make sure your accounts are secure so that they can’t be hacked and used against you.

• Learn more about managing your online reputation in Google’s Safety Center (www.google.com/safetycenter/families/manage/).

Assign the “To share or not to share?” exercise (pages 28 and 29). Have participants complete the exercise individually or in small groups. Do not advance to the next slide until participants are finished with the exercise. Answer key is on page 30.

FAMILY-FRIENDLY INTERNET (10 min)

Learning objective: Understand how to manage your family’s online activity and protect them from inappropriate Internet content or unwelcome communications.
Key points (slide 15):

- It's possible for your family to take advantage of everything good the Internet has to offer while also limiting their exposure to anything inappropriate or unwelcome.

- Parental controls—settings that allow you to decide what content is accessible to your child, how much time your child can spend on a website or app, which message boards or chat rooms can be visited, which videos can be watched, etc.—are important tools for managing and monitoring your family's online activity.

- In addition to using technology to protect your family, it's important to talk to your kids about being safe online and to agree on what is allowed and what isn't.

Questions to generate discussion:

- Do you worry about your children—youngsters to teens—being on the Internet? Why? What are your concerns?

Introduction: Like the real world, the Internet is neither all good nor all bad. As a parent, you want to allow your child to be able to enjoy all the best that technology has to offer while also protecting them from anything inappropriate or unwelcome. By taking advantage of the technology tools available, talking to your children about staying safe online and monitoring their activity, you can greatly reduce the chances of your family having a negative Internet experience.

Go over slide notes.

Slide notes: Take precautions to ensure that your family can take advantage of what the Internet has to offer while avoiding anything that is inappropriate or unwelcome.

- Many Internet service (ISP) and content providers offer parental controls—settings that allow you to decide what content is accessible to your child, how much time your child can spend on a website or app, which message boards or chat rooms can be visited, which videos can be watched, etc. Take advantage of parental controls wherever available. Learn more about parental controls from the Family Online Safety Institute (www.fosi.org/good-digital-parenting/) and in the Google Safety Center (www.google.com/safetycenter/).

There are also stand-alone parental control software programs. Some cost money, but one free one is Qustodio (www.qustodio.com). Common Sense Media provides reviews and ratings for kids' websites (www.commonsensemedia.org/website-lists).

- Talk to your children about how to be safe and responsible online. Set clear rules about which sites they can visit and with whom they can communicate. "Friend" your children—make sure you can see what they are sharing on social media, and also what others are sharing with them. Make clear that it's not okay to give out their name, address or phone number or to go alone to see someone they "meet" on the Internet. Promise not to punish them or take away Internet access if they tell you of inappropriate communications. Also let them know it's not ok to share their passwords for social networking and other sites with friends; accounts could be compromised and personal information stolen. Check out the tips at OnGuardOnline.gov (www.onguardonline.gov/topics/protect-kids-online), StaySafeOnline.org (www.staysafeonline.org/teach-online-safety/), Microsoft's YouthSpark (www.microsoft.com/youthspark) and SafeKids.com (www.safekids.com/safety-advice-tools). SafeKids.com also offers a "Family Contract for Online Safety"—signed pledges for kids, teens and parents (www.safekids.com/family-contract-for-online-safety/). Report harassment and predatory behavior to the proper authorities, which may include school officials, local police or the CyberTipline (www.missingkids.com/cybertipline/ or 800-843-5678).
ONLINE MARKETING AND DATA COLLECTION (10 min)

Learning objective: Understand how you can gain greater control over the collection and use of your personal information by websites and apps.

Key points (slide 16):

• Many online companies collect users’ personal information. Some companies use the data to customize the user experience, some use it to tailor their marketing messages and some sell it to third parties.
• A company’s privacy policy or data use policy tells you how your information is collected and used.
• Federal law (COPPA) prohibits companies from collecting information from children under the age of 13 without parental consent.
• There are things you can do to exercise some control over who collects your data and how they use it.

Questions to generate discussion:

• Why do you think websites and apps collect users’ information? Have you seen evidence that your information has been collected? How do you feel about that?
• Have you ever read a website or app’s privacy/data use policy? If no, why not? If so, did it influence your decision to use the website or app? Do you think you can trust companies to abide by the policies they post? Why or why not?

➡ SLIDE #16

Introduction: Many websites and apps collect at least some information about users in order to enhance functionality—for example, “remembering” that you placed that home-team baseball cap in your shopping cart. But some sites and apps collect more than you might be comfortable with and use it in ways that you wouldn’t approve of. While you probably can’t gain total control over when and how your personal information is collected and used, there are steps you can take to gain greater control.

Go over slide notes.

Slide notes: Many online companies collect users’ personal information. Some companies use the data to customize and enhance the user experience—such as suggesting movies and books you’d like—while others use it to tailor their marketing messages to appeal to people of similar interests. Still others—known as data brokers—collect data about consumers to sell to third-party marketing firms and other companies that use it to target ads and offers. You can exercise some control over who collects your data and how they use it.

• Reputable companies are transparent about how they use your information and they offer you choices about what to share and what you want to keep private. Read the company’s “Privacy Policy” or “Data Use Policy” to learn how and when the site or app collects, uses and shares your personal information. If you’re not satisfied with its practices, look for a different site or app that allows you more control.

• When appropriate, activate the “Private browsing” function in your web browser, which allows you to surf the Web without the browser saving information about which sites and pages you’ve visited, and use a pop-up blocker to avoid the opening of unwelcome advertising windows. (Be aware that activating certain privacy tools can hinder some desirable functionality, such as a retail website remembering what is in your “cart” or
“shopping bag.”) Think twice before clicking a banner ad or pop-up window. Click the X in the corner of the window (usually upper right-hand side) to get rid of it. Consider whether or not there is a good reason to provide more information than the minimum that is required (often indicated by an asterisk) to register for or use a website, app or service. Share the least amount of personal information possible. Understand that anytime you give up your personal information to an unvetted source—even in response to seemingly innocent quizzes or to participate in games—it can be used in ways you don’t like.

• If you have children, instruct them not to reveal private information at websites they visit. The Children’s Online Privacy Protection Act (COPPA) requires sites to obtain parental consent for the collection or use of any personal information from children under 13. Report violations to the Federal Trade Commission (www.ftccomplaintassistant.gov or 877-FTC-HELP).

RESOURCES (5 min)

Learning objective: Know where to go to find more information about protecting your privacy and personal data online and on mobile devices.

➡ SLIDE #17

Introduction: There are many resources available to help consumers learn more about being safe online and when using their smartphones and tablets. The free resources on this slide are offered by sources you can trust. You can find many more resources by following some of the links that these resources provide.

Go over resources on slide per slide notes. (Note: If you can project your computer screen, visit one or more of the sites to show participants what they will find.)

Resources

- Federal Trade Commission (FTC) (www.consumer.ftc.gov)
- OnGuardOnline.gov (www.onguardonline.gov)
- Family Online Safety Institute (www.fosi.org/gooddigitalparenting)
- Privacy Rights Clearinghouse (www.privacyrights.org)
- Google (www.google.com/safetycenter)
- Consumer Action (www.consumer-action.org)

Slide notes: There are many reputable sources of free, high-quality computer and mobile device safety information.

- The Federal Trade Commission (FTC) (www.consumer.ftc.gov) works to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. The agency offers a lot of information about computer, online, mobile device and app security (www.consumer.ftc.gov/topics/computer-security) and keeping kids safe online (www.consumer.ftc.gov/topics/kids-online-safety).
- OnGuardOnline.gov (www.onguardonline.gov) is the federal government’s online one-stop-shop to help you be safe, secure and responsible online. It is managed by the FTC, in partnership with more than a dozen other federal agencies.

- The Family Online Safety Institute (www.fosi.org) offers online advice, tips and tools to empower you to confidently navigate the online world with your kids. You can sign up for email updates and tips, too.

- Privacy Rights Clearinghouse (www.privacyrights.org) is a free, non-profit source of extensive information on privacy, including online privacy, smartphone privacy, children’s online safety and identity theft.

- Google’s online “Safety Center” (www.google.com/safetycenter) offers simple safety tools and information about staying safe on Gmail, Chrome, YouTube and other Google products. Many of the safety tips are applicable to the Internet and mobile technology in general.

- Consumer Action (www.consumer-action.org) offers free consumer education publications on a wide variety of personal finance, credit, housing and privacy subjects, including topics such as Internet safety, online banking and social media privacy.
QUESTIONS AND ANSWERS (5 min)

**Preparation:** Review the *Put a Lock on It* fact sheet.

Open the floor to questions. If time is short, offer to take additional questions after the class or at another time.

WRAP-UP AND EVALUATION (5 min)

➡ SLIDE #18

See page 31 for the course evaluation form and instructions.

Thank participants for joining you today 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 everyone to attend.
Activity: Are you cyber savvy?
Choose the correct word or phrase from the four options below each statement.

1. It is safest to use one of these when shopping online.
   a) a smartphone     b) a debit card     c) a tablet (computer)     d) a credit card

2. A strong one of these protects your accounts from being accessed by third parties.
   a) smartphone case   b) work ethic   c) password   d) spam filter

3. Set your mobile device to do this automatically when it’s not being used.
   a) lock   b) ring   c) delete your Contacts   d) restart

4. It’s important to do this when you’re finished using a financial app.
   a) reset permissions   b) email bank to confirm transactions   c) restart the device   d) log out, close app

5. Shopping or banking with this type of Wi-Fi connection can leave your information vulnerable.
   a) a weak one   b) a public one   c) a strong one   d) a spotty one

6. These digital communications are not always encrypted, so it’s best not to send sensitive data this way.
   a) email and text messages   b) phone calls and mail   c) personal conversations   d) telegrams

7. This in the browser address bar is one way to tell if a shopping or banking site is secure (encrypted).
   a) http://   b) https://   c) a key icon   d) a “smiley face” icon

8. Some attachments and downloads contain this.
   a) the secret to life   b) malware   c) spam   d) money

9. 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.
   a) delete it   b) send it immediately   c) send only your mother’s maiden name   d) turn off the device

10. Before downloading an app from an unknown source, you should do this.
    a) read the app description   b) vet the app   c) call the FTC   d) hope for the best

11. A strong password should be this long.
    a) at least 15 characters   b) at least 3 characters   c) at least 8 characters   d) 8 characters or less

12. It’s important to set your antivirus/antimalware/antispyware software to do this automatically.
    a) install software updates   b) self-destruct when a threat is detected   c) beep loudly   d) restart

13. Special software can help you do this if your mobile device is lost or stolen.
    a) calm down   b) get a new device   c) put out an APB   d) locate/lock/erase
Answer key: Are you cyber savvy?

1. Answer: a credit card
   If something does go wrong, a credit card offers greater protection—$50 maximum consumer liability (oftentimes $0) and the right to dispute charges and withhold payment during the investigation—against fraudulent transactions than a debit card does. Liability for unauthorized use on a debit card can be much higher, depending upon when you report the loss. And since debit cards are linked to your bank account, a thief could wipe you out, at least temporarily.

2. Answer: password
   A password is your first line of defense against intruders. A strong password—while not foolproof—is a reasonably effective way to protect your accounts.

3. Answer: lock
   Set your phone to lock after a few minutes of inactivity and require a passcode (or thumbprint, depending on the version) to unlock. This renders the phone useless to anyone who finds or steals it.

4. Answer: log out and close the app
   Always log out and close your apps. This prevents anyone who accesses your phone from being able to get into your accounts.

5. Answer: a public one
   Because you can’t always be sure that an outside network is encrypted, it’s safest to use your wireless carrier’s network rather than public Wi-Fi for shopping or banking when you’re away from home.

6. Answer: email and text messages
   Never send sensitive personal information such as a Social Security number or account number via email or text message. Only provide this type of information via secure website, by phone or in person.

7. Answer: https://
   The “s” in https:// stands for “secure.” It means that the data being sent is encrypted, or scrambled, so it is much more difficult for a hacker to steal. You might also see a padlock, or the address bar itself might turn green when you enter a secure website.

8. Answer: malware
   Attachments, software and downloads often contain undesirable software (malware or spyware) or a virus. Only open attachments and download files and software or apps from trusted sources.
9. **Answer: delete it**

   Never respond to email or text messages asking you for sensitive information. Legitimate businesses and government agencies typically will not ask you for this information at all, and they’ll never ask for it via email, text message or phone.

10. **Answer: vet the app**

   It’s not enough to just read the app’s description. Start by getting your apps only from trustworthy sources, and then read the reviews to find out if anyone has had problems. If you can’t confirm an app’s legitimacy and commitment to your safety and privacy, find a different app.

11. **Answer: at least 8 characters**

   Anything less than eight characters is too weak. Some experts are now encouraging consumers to shoot for 10 characters.

12. **Answer: install software updates**

   Software updates typically include improvements in security. To avoid being unprotected against new viruses, malware and other threats because you forgot to run the update, set your software to update automatically.

13. **Answer: locate/lock/erase**

   Apps such as Find My iPhone (Apple) or Android Device Manager allow you to find your device if you’ve misplaced it, or remotely lock it or delete your data if it’s lost or stolen so that whoever ends up with your phone can’t access the data.
Activity: Something’s phish-y!

In the email messages below (actually received by Consumer Action staff), identify any tip-offs that the message might be a phishing attempt. Be prepared to discuss your observations. (Note: Names and personal email addresses have been redacted to protect individuals’ privacy.)

From: Amazon Prime Members but@loveovenamazon.in
Subject: REMINDER: You Have (1) Account Message - $100 Credit Added to Your Account - Member: email macro
Date: June 25, 2015 at 7:21 PM
To: monicast@earthlink.net

Congratulations - You've Been With Amazon For 1 Year!

As a thank you we've gifted you $100 that can be spent on anything you'd like at Amazon.com. (Expires 12/31/15)

Shop Now

Dear Shopper,

Summer is just around the corner! We want to remind you that you can use your Amazon.com Store Card to get your favorite electronics, lawn and garden, apparel items, and more!

Click Here Now to Grab Your $100 Reward!

Get 6 Months
Special Financing*
on all purchases of $149 or more

Get 12 Months
Special Financing*
on all purchases of $599 or more

Get 24 Months
Special Financing*
on qualifying purchases

Click here to see all qualifying items
From: Southwest Airlines  aas@flyrighttonight.in  
Subject: REFUND ISSUED: A $100 Credit Has Been Added to Your Account - Please Confirm:  
Date: June 25, 2015 at 12:09 PM  

One (1) Credit Issued - Credit #39511

Dear Traveler,

Due to a recent change in our billing system there has been a number of flights that were overcharged. We’re issuing a voucher of $100 for any Southwest flight to any domestic location.**

Please be sure to click on the image of the voucher below to apply the $100 Southwest voucher to your account.

We’d also appreciate it if you could respond to our customer service survey. Upon completion of the survey we will add an additional $50 voucher to your account as a thank you for your participation.

Enjoy Your Flight!
-Southwest Airlines

Click Here

9 07 12345 00012 001960

**Excluding Puerto Rico

This email you’re viewing is an online advertisement. To unsubscribe from our email list you can click here now and you will be removed within 10 business days but likely sooner. You can also reach us via regular mail at: 1090 Fairfax Avenue #1D, Los Angeles 90078.
Twila Rutherford used Dropbox to share some files with you,

We just need to verify your email address before you can view files and folders.

Verify your email

NOTE: You are accessing a highly secured important Document.

Enjoy,
- The Dropbox Team
To view the shared document, you are required to Login with your email address below:

Email Address:  

Email Password:  

Sign in
Answer key: Something’s phish-y!

Amazon email:
• The sender’s email address is but@loveovenamazon.in—a dead giveaway that the email is not from Amazon.
• The email is blurry, or fuzzy…not crisp. The font seems larger than typical, and the capitalization and punctuation seem off (all initial caps in the first line, for example). The wording also seems off—for example, “grab” your $100 reward, and “lawn and garden” doesn’t work in the list unless there is another word after it, such as “equipment,” “tools,” etc.
• In the upper right-hand corner, it says “For your account ending in: 059.” Unless you happen to have an account ending in 059, this is a clue that the email is bogus.

Note: While the logo, card image and merchandise images are accurate, they are easily copied from the real Amazon website and are not any indication that the email is legitimate.

Southwest email:
• Like the Amazon email, the Southwest email displays a “From” address that obviously does not belong to Southwest Airlines.
• The message contains bad grammar (“…there has been a number of flights…” instead of “…there have been a number of flights…”), a misspelling (“completetion” in the third paragraph instead of “completion”), unnecessary capitalization (“Enjoy Your Flight!” instead of “Enjoy your flight!”) and non-standard business language (“…within 10 business days but likely sooner”).
• The physical address in the unsubscribe section seems odd for a large company. Checking it online does not provide any results for that street address—a warning sign.

Note: Clicking on either the Amazon or Southwest messages landed us on a warning page that said “It’s a trap! Reported phishing or malware site” and informed us that the site was blocked by our Internet service provider (ISP). (Incidentally, the person who received this email has never flown on Southwest.)

Dropbox email:
• The first and most obvious tip-off that this is a phishing email is the mistaken use of a comma rather than a period at the end of the first sentence (“….to share some files with you,”).
• The next tip-off is the unusual characterization that “You are accessing a highly secured important Document.” First, how does Dropbox know what the person is sharing—it might be something that is not at all “important.” Second, that unusual wording (something you don’t generally see in a professional email) seems like it is trying very hard to pique your interest and get you to take the next step. Third, there is no reason for “Document” to be capitalized at the end of the sentence.
• The last tip-off is the “Enjoy” at the end of the email. That is an odd sign-off for a professional email, especially considering that the sender, if legitimate, wouldn’t know what kind of files were being shared with you—they could be legal documents, tax records, etc.?

Dropbox spoofed webpage:
The Dropbox phishing email takes you to this webpage, which does not have any glaring tip-offs that it is spoofed (except perhaps the unnecessarily capitalized “Login” in the instructions). The one big clue that this is a spoofed webpage is that it asks you for your email address and password for no good reason. (How would Dropbox verify your identity from your email address and password since it’s not related to your email account and presumably wouldn’t already have this information to compare your entry against?)

Note: A number of the recipient’s friends fell for this phishing attempt because the email (coincidentally?) arrived within days of her returning from a trip; friends thought she was sharing photos from her travels.
**Activity: To share or not to share?**

For each post, determine whether or not the communication is safe and smart to share via social media or not, and why.

---

**Joe Davis**  
@JoD

Anyone up for another Friday “sick out”? Can’t stand the thought of work today.

---

**Lisa Welch**  
5 minutes ago

Date night at Chez Pierre ([www.chezpierre.com](http://www.chezpierre.com)) tonight! And no babysitter bill now that the kids are finally old enough to stay home alone.

---

**Chris Fleming**  
Executive Assistant at AA Products Inc.  
San Francisco Bay Area | Manufacturing

**Experience**  
Executive Assistant  
AA Products Inc.  
2014 – Present (1 year)

Provide project management, office administration and event planning for disorganized CEO. Provide regular backup to undertrained bookkeeping staff. Assist HR in filling vacant positions due to high staff turnover. Seeking new position because I found out in a memo that the company is being sold.
Felicity Dawn Lee
Shared publicly – Yesterday 6:14 PM

Get a load of this pic of my mother with her bridesmaids the night before she married my dad—when she was still Sarah Jones.

**************

Dee Dee
@DD

Oh no…started smoking again over the weekend after six months of no cigs! Need to get back on the wagon (@quitsmoking).

**************

Frank Foley
14 hrs

____________________________

Lighten up…if you thought that joke was sexist, you just don’t have a sense of humor.

**************

LynnD’mato

Janet, you’re a lifesaver! Thanks again for “helping” me with that term paper.
Answer key: To share or not to share?

Tweet (Friday “sick out”): This would look bad not only to your current employer, who might hear about your playing “hooky” from a co-worker who is your social media friend, but also to any prospective future employer who might check your social media activity during the hiring process.

Facebook post (Chez Pierre): Sharing that your children are home alone, along with exactly where you’ll be and when, is risky. Another option is to share only that you and your spouse will be having a date night. You could also share the information about your evening after you get home.

LinkedIn: In addition to making your boss look bad (disorganized), the entire bookkeeping staff look inept (undertrained) and the company look like a bad place to work (high staff turnover), you also risk getting fired or worse for leaking a memo about possibly confidential company finances (a sale).

Google+ post: This post is a problem because you have revealed your mother’s maiden name—a commonly used identifier for financial and other accounts. Delete “when she was still Sarah Jones” and this post would be safe.

Tweet (smoking): One of the benefits of social media is being able to solicit others for support and advice, but in this case you should make absolutely sure that nobody outside your close circle of friends could see the tweet. Your smoking could be an issue for some, such as your health and life insurance provider (higher risk, so higher premiums or no coverage) or your landlord (smoking in a non-smoking property).

Facebook post (sexist joke): This could raise a red flag for a prospective employer, college admissions officer or anyone else trying to gauge your character. The issue is not only this response, which shows a lack of awareness and empathy, but also the originally posted joke, which at least one person found offensive.

Tumblr post: This could look to your teacher, a college admissions officer or other education professional like you had someone else write your term paper—particularly with “helping” in quotes. Either don’t post about this at all, or leave it at something like “Janet, thanks a lot for your input on my project. You’re the best!”
Training evaluation: *Put a Lock on It*

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 my role in protecting my own privacy and data online.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

2. *I am more aware of the specific tools and practices that I can use to stay safe online.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

3. *I better understand how to vet websites and apps to avoid problems.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

4. *I feel better prepared to spot and avoid scams, malware and other online threats.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

5. *I feel better able to distinguish between appropriate social media sharing and oversharing.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

6. *I am more aware of ways to protect my children online.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

7. *The instructor was well informed.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

8. *The materials I received are easy to read and understand.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

9. *I would like to attend another class like this.*
   - Strongly agree
   - Agree
   - Disagree
   - Strongly disagree

On a scale of 1 to 10 (10 being the best), how would you rate the training? ______________

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

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

---

*Thank you for attending!*