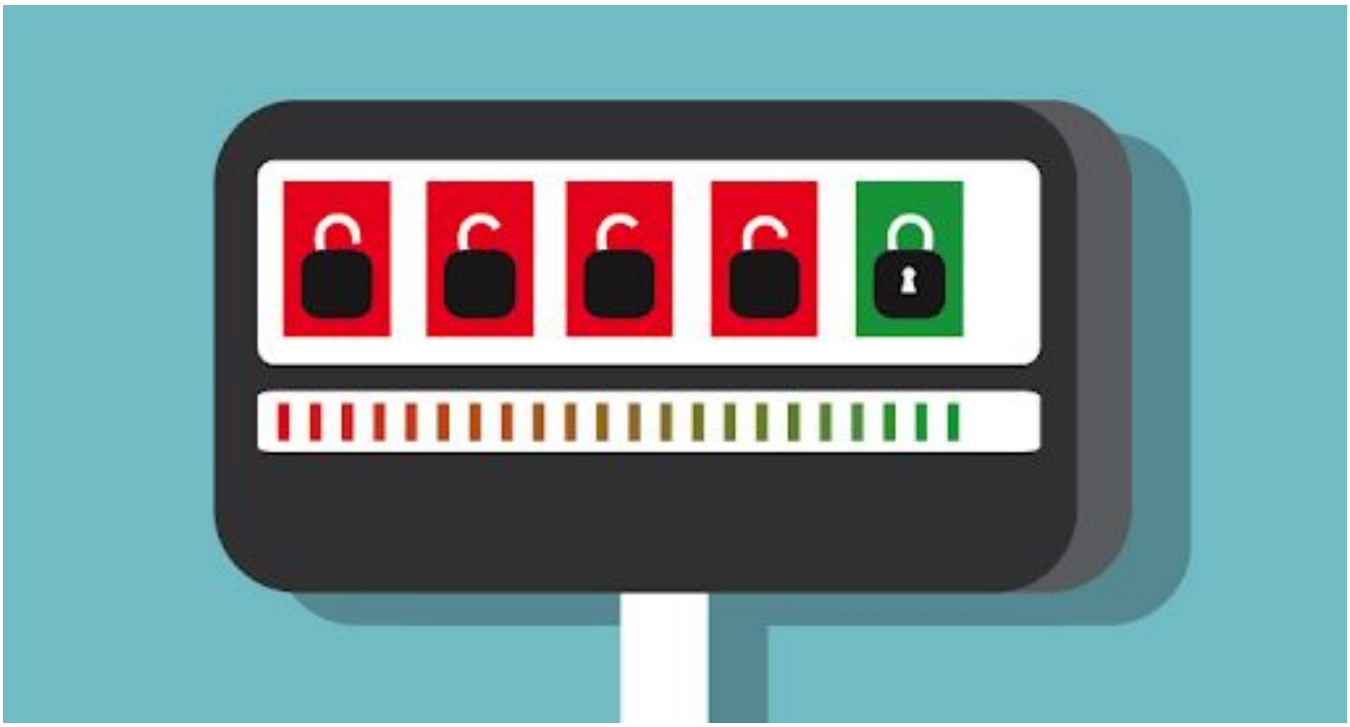

Protecting Your Online Privacy: Encryption and Phishing

Organizer's Guide

V1.3.0

Consumer Reports' Community Workshops

Thank you for volunteering to host a workshop on online privacy!

For over 80 years, Consumer Reports has been dedicated to working side by side with consumers for truth, transparency, and fairness among products and retailers. As we shift toward a more digital world, we are seeing new technologies, products, and services entering people's lives every day, and new concerns are emerging.

Consumer Reports is dedicated to bringing the power back to consumers and having them feel in control of their digital lives. But we can't do it alone. That is why Consumer Reports relies on its community (that's you!) to help us inform and empower citizens across the nation to protect themselves online. We can't say this enough: Thank you for helping us create a more informed and safer world.

Introduction to the Organizer Guide

We know that running an event can be hard. We also know that teaching online privacy can be confusing. We don't expect you to be an expert in either! That's why we've created this guide—to help you feel prepared, regardless of your previous experience. Read the guide carefully to capture the tips, tricks, and trusted methods we've listed that are sure to make your event an effective and fun gathering for all those involved.

In this guide there are multiple activities that teach about how to create secure passwords in easy-to-understand and hands-on ways. Activities have estimated times and step-by-step instructions to help you facilitate the workshop. The instructions are meant to act as frameworks and can be adjusted to make the event feel more natural. Make the content your own. So *don't* use it like a script, but *do* personalize it and *do* focus on making it discussion-based. We estimate that the entire module will take 80 minutes to complete, but we recommend adding a break and adjusting times where needed.

If at any point you need additional support organizing your event or teaching activities, contact the CR team at community@cr.consumer.org. We are here to help you every step of the way.

Additional Documents

Participant Workbook: The participant workbook should be given to every participant in your workshop and will serve as their activity book. The workbook also contains a glossary of key terms.

PowerPoint Presentation: This PowerPoint contains the complete run of show, key points, and visual aids. This is optional, and you are not required to use this presentation.

Organizer Toolkit: The Toolkit contains details on how to organize and facilitate your workshop, as well as links and templates that can be easily adapted.

Welcome and Introduction

SUMMARY	Facilitators will introduce the workshop and an icebreaker activity.
OBJECTIVES	➔ Introduce facilitator(s) and participants. ➔ Set ground rules. ➔ Hold an icebreaker discussion.
ESTIMATED TIME	20 minutes
ACTIVITY TYPE	Group discussion
PARTICIPANT HANDOUTS	Page 1

STEP 1: Introductions

SLIDES 2 through 5

5 minutes

- ➔ Welcome participants to the workshop and introduce yourself. Participants should also introduce themselves at this time.
- ➔ Discuss why you have organized this event and what digital privacy means to you. *(Note: this should be and feel personal. Make sure participants know why **you** care about this topic. If you need help, use the data on digital privacy that we've gathered below.)*
- ➔ Explain what Consumer Reports is and why the organization cares about digital privacy.
- ➔ Review the agenda for the day and share why the topic you chose is important—what are the threats and issues we face because of it?
- ➔ Describe the goals for the workshop. It is helpful to list topics covered in other modules (such as passwords and data management) and explain that they might come up in discussion but are taught in greater detail in other modules.

Why Digital Privacy?

- We are increasingly surrounded by new technologies, and while they are fun and convenient to use, they are constantly collecting or sharing personal details of our lives.
- As citizens, it is important for us to stay informed and in control of the technology we use so that we can stay safe among emerging threats.
- In the wrong hands, our personal data can be used against us—to coerce us into making decisions or paying increased prices based on our preferences, or exploit us into giving away sensitive information or money, among other behaviors.
- Along with understanding how we share our data and keep it safe, we must also hold organizations and government responsible for ensuring safe and equitable data practices, so we can continue to enjoy the opportunity of the digital world.

Consumer Reports and Digital Privacy

- Consumer Reports has been representing consumer interests and rights for over 80 years as an active stakeholder in improving the quality and policies surrounding the foods we eat, the products we use, and the services we purchase.
- As we take on the challenges of the digital world, Consumer Reports has launched an initiative dedicated to solving the problem of the harm consumers face when using technical products and services. Our goal is to shift the power back to consumers and allow them to feel in control of their digital lives.
- Having already advocated for better policies, like the California Consumer Protection Act, and completed investigations on facial recognition tools, Consumer Reports feels confident that it can continue to support consumers in the digital world to ensure fairness, safety, and transparency.

Workshop Goals

The goals of these community workshops:

- Discuss important consumer information on a variety of topics—today, we're here to talk about digital privacy and how people interact online.
- Share how you can also run these workshops in other community settings.
- Have fun!

STEP 2: Ground Rules

SLIDE 6

🕘 5 minutes

➔ Discuss the importance of ground rules at events.
➔ Share a list of ground rules that will allow for an open, safe, and fun environment.
➔ Ask participants if they have questions or if they wish to add to the ground rules.

Importance of Ground Rules

- It is important to set ground rules at events because it helps us shape how we will collaborate with each other and create a shared space where everyone feels open to contributing.
- Topics such as privacy can be very personal, and attendees can have a range of experiences, including some negative or conflicting ones.

Sample Ground Rules

- Listen actively—respect others when they are talking.
- We are all here to learn. Everyone's opinion is valid and important. There are no bad ideas.
- The conversation is not meant to discredit any person, organization, group, demographic, or gender.
- Topics like privacy can be difficult for many reasons. Talk from your own experience and be open and empathic to others' opinions.
- Your privacy means protecting your personal information. Share stories and information you are comfortable with, while not disclosing sensitive information about your accounts.
- The intent is to participate to our full capabilities and to work together.

STEP 3: Icebreaker

 **SLIDE 7**

 **WORKBOOK 1 and 2**

🕘 10 minutes

➢ Instruct participants to get into pairs, preferably with someone they don't know.
➢ Ask the pairs to discuss answers to each question.
➢ Bring the group back together for a quick debrief and invite participants to share highlights of their answers if they feel comfortable.

? Questions

- How many products do you own that are connected or could be connected to the internet?
- What excites you about the future of technology?
- What might you find scary or unfair or strange about technology?

Debrief

- Who has the highest number of products that connect to the internet?
- What did individuals find exciting about technology?
- What did individuals find scary or unfair or strange about technology?
- Did you and your partner have similar answers?

Keeping Accounts Protected

Activity 1: The Key to Encryption

SUMMARY	In this activity, facilitators will discuss and teach how to use encryption
OBJECTIVE	➔ Learn about encryption and how to enable it on platforms or with personal data.
ESTIMATED TIME	25 minutes
AUDIENCE	Beginner level
ACTIVITY TYPE	Group discussion, individual work
MATERIAL	Pens

STEP 1: Sending Personal Information

 **SLIDES 9, 10, and 11**

 **WORKBOOK 3**

5 minutes

➔ As a group, discuss what type of personal information you want to secure when sending it across the web. Once the group has exhausted the list, share any of the below that weren't mentioned.

Sensitive Information Shared Online

- Credit card information
- Banking information
- Numbers that can be used to identify you (e.g., phone number or Social Security number)
- Personal details or documents (e.g., passport)
- Private company information
- Messages to others

- Health/hospital information

➔ Discuss how much private data the group shares on the internet and where participants feel most and least secure sharing private data.
➔ Ask participants how they secure their information when sending private or sensitive details on the web. Discuss some of the common practices that participants can use to protect themselves.

Practices for Sending or Storing Sensitive Details

- **Look for the padlock icon in the browser beside the URL.** This icon means that the connection is secure and that the information you submit to the site cannot be intercepted by a bad actor. At times you might see this icon with a red strikethrough or yellow triangle warning sign; this indicates that the connection is only partially protected.
- **Seek out sites with addresses that start with "https" (vs. "http").** The "s" stands for "secure," and this addition to the URL indicates that your communications with the site aren't seen by unknown third parties.
- **Engage with trusted platforms.** Use sites and services that are known and provide information on keeping your information secure. Even if you see a security padlock or are using https, it doesn't mean you are protected from the company using your data in malicious ways. Look for text on the site or do a quick search online to gauge reviews from others.
- **Enable passwords or security questions.** Some sites, particularly banking ones, will allow you to enable passwords or security questions so that only people with the select information can accept transfers or open documents.
- **Lock personal devices.** Use passwords that only you know on your mobile devices and personal computers, so others can't access your information when these devices are left unattended or misplaced. Make sure the passwords are hard to guess; don't make them "0000" or "password."

STEP 2: Crack the Code Activity

SLIDES 12 and 13

WORKBOOK 4 and 5

15 minutes

- ➔ Have participants turn to their workbooks and complete the “crack the code” activities.
- ➔ Once they crack the code, have them complete the next activity to create a secret message.
- ➔ Ask participants to swap their secret messages with another individual and crack the patterns used to code the new message.

? Crack the Code Exercise

The objective of the activity is to learn the basics of encryption, and what it means to alter a message and create a code so that only the sender or recipient can translate and access it. Codes and cyphers have been used for a long time to encrypt communication and keep it secure during transportation.

? Suggested Prompts

- Were you able to decode the secret message? What did it say?
- Were you able to solve the numeric lock? What was the code?
- Was your partner able to crack your message and pattern? Did he or she find it easy or difficult to see the pattern used?
- Which ways did people code their messages to make them hard to crack?
- Have you done an activity like this before? How is it similar to morse code or other cyphers?

Answers

The secret message is:
piece of cake
(The workbook shows the secret message backward.)

The number to open the lock is:
597
(The workbook hints help solve this riddle. If participants are having trouble, it is usually easiest to start with the section that says “nothing is right” and work backward through a process of elimination.)

➔ Discuss as a group how this is the basis of encryption and securing information online. If any participants know the definition of encryption and how it works, ask them to describe it to the rest of the group.

? Suggested Prompts

- Has anyone used codes or cyphers to protect sensitive information in the past? How do we use them online and offline?
- Does the word encryption sound familiar? Where have you seen it used online?
- What does it mean when you see text saying, “his message is encrypted”?
- If your data is encrypted, can it still be hacked?

Encryption

- Encryption is the process of altering or changing a message to hide its meaning. The message is changed so dramatically that it is unreadable unless you know how it was edited.
- Usually, this process has two important components: something that encrypts and something that decrypts. There are many such components used in websites, phones, radio frequency identification (RFID) tags, etc. Many modern encryption and decryption methods rely not on the complexity of the process (they’re actually quite simple) but on the mathematics behind it to provide simple, noncontextual security.
- When private data falls into the wrong hands through hacking or other means, this is often referred to as a “breach.” However, often the data is encrypted, and there are standard encryption practices that prevent that data from being decrypted when a breach occurs—the information is still protected.

- Unfortunately, it is possible for hackers to break encryption in some cases, solving the code and accessing your personal information—but that's harder to do and can take time.

STEP 3: Encrypting Files and Tools

 **SLIDES 14 and 15**

 **WORKBOOK 6**

10 minutes

➔ As a group, discuss how to encrypt your files or data. Have participants encrypted their information in the past? If so, what methods have they used?
➔ Discuss various methods of encryption in everyday use. Write the methods and tools in a visible place for participants to see.

Ways to Encrypt Your Files or Data

- Enable encryption and/or two-factor authentication in your settings.
- Encrypt your hard drive or USB keys that store sensitive information.
- Encrypt a specific file that contains personal information.
- Use encryption tools to safely send information to others.

Encryption Tools

- There are many free tools available online that can be used to encrypt single files or documents. These can be valuable when you have to send your personal data, such as banking info, Social Security number, or passport, to others. These tools can be particularly useful if the platform or receiver appears less secure and you want to ensure that your information remains private.
- These tools give you the option to add a password to your files, and the information can be accessed only by those with the password. You can share that password with anyone you wish to view the file.
- Examples of free online tools that encrypt individual files include AxCrypt and 7-Zip.
- Examples of free online tools that encrypt entire hard drives include BitLocker, FileVault 2, and VeraCrypt.
- Examples of messaging tools that use encryption include iMessage, Signal, Viber, and WhatsApp.

Activity 2: Phishing

SUMMARY	Facilitators will discuss how to create strong passwords and security questions, and what tools are available.
OBJECTIVES	➔ Understand how security questions can be uncovered. ➔ Know how to pick and answer security questions.
ESTIMATED TIME	20 minutes
AUDIENCE	Beginner level
ACTIVITY TYPE	Individual quiz activity and group discussion
MATERIAL	Pens

STEP 1: What Is Phishing?

 **SLIDES 16 and 17**

 **WORKBOOK 7**

10 minutes

➔ As a group, define phishing.
➔ If you have a personal story about a phishing attack, tell participants. There are also many examples available online and a sample one shared below.
➔ Encourage participants to share their own stories if they feel comfortable. Remind participants that phishing attacks can be sophisticated and that even the most prepared individual can be a victim.
➔ If the group is unable to share stories, use the example story we've listed below.

Phishing Defined

- Phishing is a process that is meant to obtain an individual's sensitive information, such as passwords, phone numbers, credit card numbers, Social Security number, and more.
- Here's a great video about someone who decided to scam the scammers: https://www.youtube.com/watch?v=_QdPW8JrYzQ

- Scammers send thousands of fraudulent emails every day and are often successful because they appear to be reputable companies. The FBI's Internet Crime Complaint Center reported that criminals made $676 million in 2017 through phishing schemes.
- Though most often occurring in emails, phishing can also take place in phone calls, text messages, social media, advertisements, and mail.
- Phishing schemes have become more sophisticated over the years and are increasing at alarming rates. In some schemes, it's hard to tell the difference between a legitimate email and a phishing email.
- While attackers send out many phishing messages hoping that at least one person will share their information, they often prey upon those with low web literacy skills who are most likely to click and enter personal information.

Phishing Stories

- In 2018, the World Cup took place in Europe and individuals around the world were eager to attend events, be updated on scores, and win prizes from sponsors. Scammers took advantage of this opportunity by sending phishing emails to many individuals in the U.S. These emails contained suspicious attachments that would download malware on an individual's computer or require an individual to respond to an unsecure email address or website that allowed attackers to steal personal and financial information. In some cases, individuals would even pay a fee in hopes of claiming prizes and tickets to games.
- Find more information on this World Cup phishing attack here.
- Read the official statement by the Federal Trade Commission on avoiding World Cup scams.

Avoiding World Cup scams

Share this page

June 25, 2018
by Andrew Johnson
Division of Consumer & Business Education, FTC

The long-awaited 2018 World Cup is underway. Fans from across the world have flocked to Russia in support of their favorite teams. Though most have already bought their tickets, many are still hoping to come across an unbeatable deal that will get them to the Cup.

While fans hope for a good deal, scammers hope for ticket-hungry fans. Here are a few tips for avoiding World Cup-related scams:

- Ignore any email that claims you've won World Cup tickets or a lottery prize to attend the Cup. The offer may seem promising, but the truth is, scammers are simply phishing for your personal information. Never open files or click on links sent by strangers. And never pay a fee to claim a prize.

- Want to read more stories? Search for popular phishing stories online and read about real attacks like Phish Phry, the tale of Walter Stephan, or Moscow's World Cup rental scam (through Booking.org).
- This story is to share extra background on phishing. If participants in the workshop have stories, don't share this one.

STEP 2: Phishing Case Studies

SLIDES 18, 19, and 20

WORKBOOK 7, 8, and 9

10 minutes

➔ Have participants read the phishing case study in their workbooks and follow the question prompts.
➔ After participants have completed the prompts, bring the group back together to discuss reactions to the case study and share their answers. Be sure to discuss how to spot the phishing scam in the case study.

Case Study Explained

This case study reviews a phishing scam that is similar to emails seen by real customers using popular banks in the U.S. Often what makes those emails look real is that they include the logo and branding of the bank, with similar email addresses and titles.

What should Taylor do in this situation?

- Taylor should not click on any links in the email or respond to the sender.
- Taylor should not dial the customer service number provided.
- Instead, Taylor can find a customer service number from an online search or on the back of his or her bank card or on mailed statements. Taylor can then call the bank directly to inquire as to whether the account has been suspended or find out about any action that has occurred.
- Taylor can also freeze the account or add extra password protection to ensure that he or she is the only one able to access it.
- If the email is confirmed to be a scam, Taylor can delete the email and either ignore it or mark it as spam in his or her inbox. Marking an email as spam notifies the email provider and potentially blocks that sender or email from being sent to others.

How do we know the email was phishing?

- The email was sent from a Hotmail account. Organizations and institutions have their own email address providers and don't send sensitive emails through email services such as Gmail, Hotmail, and Yahoo (unless it is a mom and pop shop). A more legitimate address could have been customerservice@trustedbank.net. Email addresses from services such as AOL, Hotmail, and Yahoo are also cause for suspicion and should be validated before responding.
- The email asks for personal details, such as your account information and password. Banks will not require this information unless you are logging in to their site.
- The email requires immediate action, which makes you feel like you have to respond quickly. This trick is used to get individuals to take quick action without consulting elsewhere or thinking further of the action.
- The site is trustedbank.eg. Most reputable sites have a URL ending such as .com, .net, or .org.
- The email contains a spelling mistake at the end. It spells "customer" wrong.

➔ As a group, discuss ways people can recognize and protect themselves from phishing scams. Write a list in a visible spot at your event.

How to Recognize Phishing Scams

- It looks like it is from a company you know or trust, though it has an old logo or information.
- It contains spelling errors, bad grammar, or unusual sentence structure.
- It asks you to update your account information by re-entering passwords and personal information.

- It uses an unfamiliar domain, such as .eg or .ie.
- When you click on the link, the URL does not match the company listed in the email.
- You have to submit payment to claim your prize.
- It includes a fake invoice.
- It says your account or service is on hold because of a billing problem.
- It includes a link that will direct you to coupons, free items, or refunds.
- It requires immediate or urgent action.

What to Do If You've Been Scammed

- If you're uncertain about whether you've received a phishing email, use a web browser to go directly to the site or search a customer service number online and make a direct call to check on the status of your accounts. If there's even the faintest shadow of a doubt, even if you think you're being silly, trust your instincts!
- Report the incident to the FTC at http://ftc.gov/complaint and the Anti-Phishing Working Group at reportphishing@apwg.org.
- Call appropriate companies, such as your bank or employer, to inform them of the attack. In some cases, it will be necessary to freeze accounts.
- Contact the company directly and inform it about the attack so that it can alert other users.
- In some cases, you might have to download antivirus software on your computer.
- Enable multifactor authentication and encrypt your sensitive information.
- Change compromised information and passwords (if possible).

Conclusion

SUMMARY	Close out your workshop with one final reflection.
OBJECTIVES	➔ Discuss what participants are taking away from the workshop. ➔ Share what participants can expect after the workshop.
ESTIMATED TIME	10 minutes
ACTIVITY TYPE	Group discussion

STEP 1: Final Comments

 **SLIDES 21 and 22**

5 minutes

 **WORKBOOK 11**

➔ If you have a small group, have everyone go around in a circle and comment on something they learned, found interesting, or will do differently as a result of the workshop.
➔ If your group is large, ask individuals to break off into pairs and discuss their reflections. Bring the group back together and ask if anyone wants to share what was discussed.
➔ Encourage the group to share any outstanding questions or comments.

? Suggested Prompts

- What is one thing you will take away from the workshop?
- How does this relate to the technology, platform, and devices you use every day?
- How will you share something you learned with someone who didn't attend this workshop?

STEP 2: Next Steps

 **SLIDE 23**

5 minutes

 **WORKBOOK 11**

- ➔ Discuss what happens after the workshop. Is another workshop planned? Where can people go for more information?
- ➔ Share ways you plan on following up with individuals. What can they expect in a post-event email? Every guide comes with links that can be shared in your email; be sure to highlight these articles now and include them in your email.
- ➔ If people are interested in **three free months of Consumer Reports** (the magazine and/or digital access), they can fill out the final page in their workbook and leave it with you.
- ➔ Ask participants: If Consumer Reports trained them to give this workshop, would they be interested in hosting a meeting like this, where they invite their friends and family or community members? Who else needs this information?
  - ◆ If so, have them indicate their interest on the last page of the workbook.
- ➔ **Bonus:** As optional homework, invite participants to contribute to the larger "herd immunity" of spam filters by going into their spam folders, finding emails that are *clearly* spam, and marking them as spam.

Resources and Links

The resources and links below are to aid your workshop. They might be helpful for you to review before the workshop and learn more about the topic, or you can share them with your participants during the workshop, or even send them to participants after the workshop.

Additional Resources

ARTICLE: How to Use Encryption: It's Easy
https://www.consumerreports.org/digital-security/how-to-use-encryption-its-easy/

ARTICLE: How to Identify a Phishing Email
https://www.consumerreports.org/consumer-protection/how-to-identify-a-phishing-email/

ARTICLE: How to Protect Yourself From Phishing
https://www.consumerreports.org/money/how-to-protect-yourself-from-phishing/

ARTICLE: How to Avoid Apple and Amazon Phishing Scams

https://www.consumerreports.org/phishing-vishing/how-to-apple-and-amazon-phishing-scams/

VIDEO: Encryption and Public Keys
https://www.youtube.com/watch?v=ZghMPWGXexs

VIDEO: Stay Safe From Phishing and Scams
https://youtu.be/R12_y2BhKbE

Encryption Tools

- Encrypt individual files free
  - AxCrypt axcrypt.net
  - 7-Zip 7-zip.org
- Encrypt entire hard drives free
  - VeraCrypt veracrypt.fr
  - BitLocker (Windows only) docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
  - FileVault 2 (Mac only) support.apple.com/en-us/HT204837
- Messaging tools that use encryption
  - Signal signal.org
  - WhatsApp whatsapp.com
  - Viber viber.com
  - Telegram telegram.org
  - iMessage for iOS users