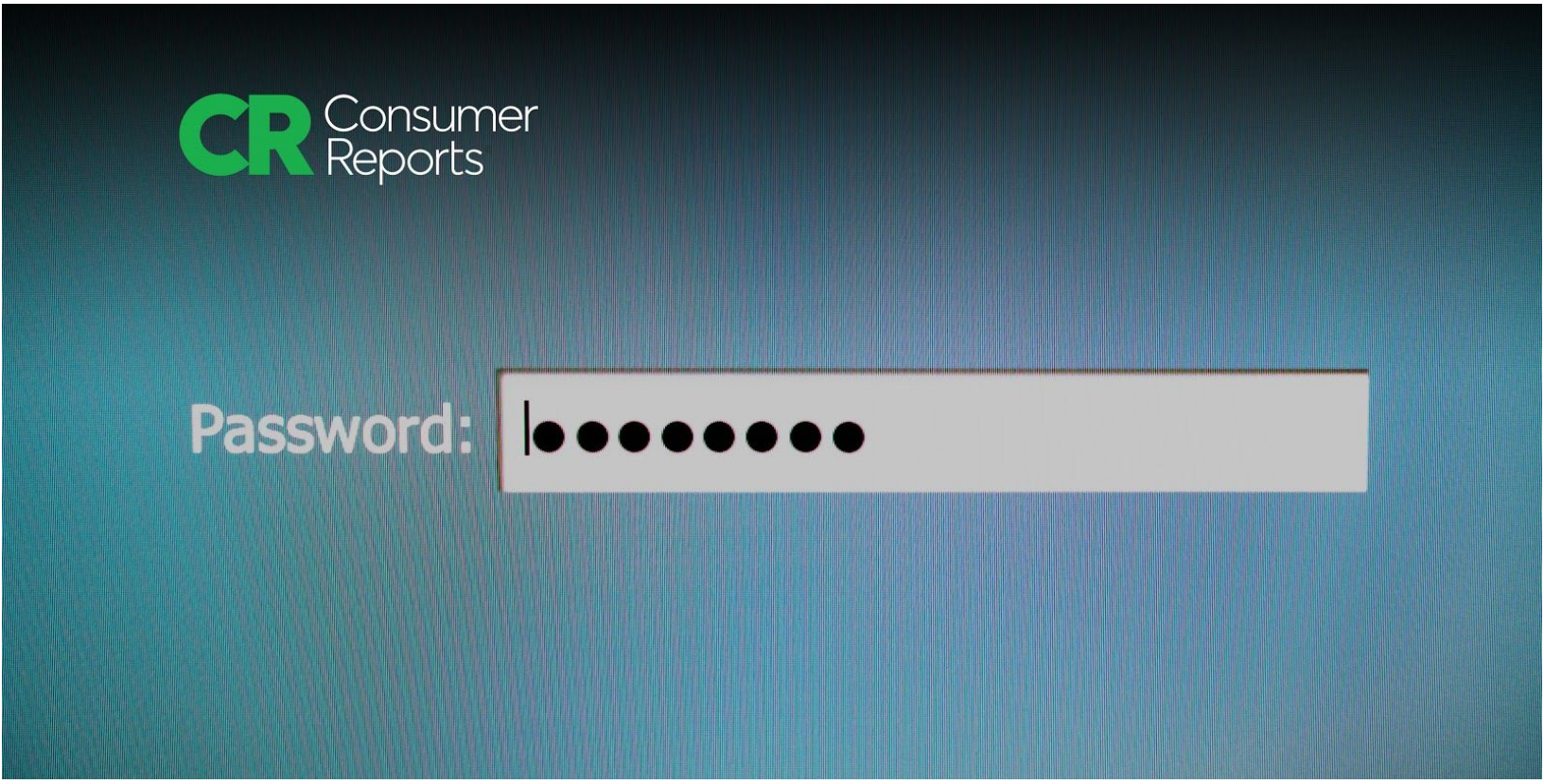


Protecting Your Online Privacy: Password Management

Organizer's Guide

V 2.1.1

Consumer Reports' Community Workshops

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

For more than 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. Though we can't do it alone. That is why Consumer Reports relies upon its community (that's you!) to help us inform and empower citizens across the nation how 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's 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 convening 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 suggested 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* make it personable and discussion-based. We estimate the entire module to 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.

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.

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

STEP 1: Introductions

SLIDES 2-5

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 who Consumer Reports is and why it cares about digital privacy.
- ➔ Review the agenda for the day and share why the topic you chose is important—what are the threats and concerns we face because of it?
- ➔ Describe the goals for the workshop. It is helpful to list other topics covered in other modules (such as encryption, phishing, data management, etc.) and identify 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 though 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, paying increased prices based on our preferences, and exploit us into giving away sensitive information or money, among other things.
- 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 that 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 more than 80 years as an active stakeholder in improving the quality and policies surrounding what 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 for the harm consumers face in technical products and services with the goal of shifting the power back to the consumers and having them 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 are to:

- 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 whether they have questions or 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

 **SLIDES 7 and 8**

 **WORKBOOK 1**

10 minutes

➢ Instruct participants to get into pairs, preferably with someone they don't know.
➢ Ask participants to discuss in their pairs answers to each question.
➢ Bring the group back together for a quick debrief and invite them 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?

Generating Strong Passwords

Activity 1: Why create a strong password?

SUMMARY:	Facilitators will discuss how to create strong passwords, security questions, and tools available.
OBJECTIVES:	➔ Learn about data breaches and the importance of setting strong passwords. ➔ Learn how to set passwords that work.
APPROX. TIME:	20 minutes
AUDIENCE:	Beginner level
ACTIVITY TYPE:	Group discussion
MATERIAL:	Pens Internet-connected devices (computers or smartphones)

STEP 1: Data breaches

 **SLIDES 9, 10, and 11**

 **WORKBOOK 3**

🕘 5 minutes

➔ Define data breaches. Discuss what happens to your password or personal information in a data breach.
➔ As a group, discuss what it means if you use the same password on multiple accounts.

What Are Data Breaches?

- There have been billions of emails, passwords, credit card numbers, and other personal information that have been stolen and released online for hackers to access. These are referred to as data breaches, and it means your account information has been taken and shared with external parties.
- Consumers and platforms have little recourse for this kind of breach. Most often, by the time we hear about a data breach our information has already been shared, and

there is no way to reverse the breach to get the data back or remove it from the internet.

- Unfortunately, there are not a lot of consumer data protection laws. That means the responsibility is left to consumers to secure their data as best as they can. CR is working to change this by advocating for more laws and data protection in state and federal levels.
- If a consumer's password is the same on multiple sites, this means that all those sites are easily hackable and malicious individuals can use that same password to gain access. There are automated programs that make this an easy and quick process.

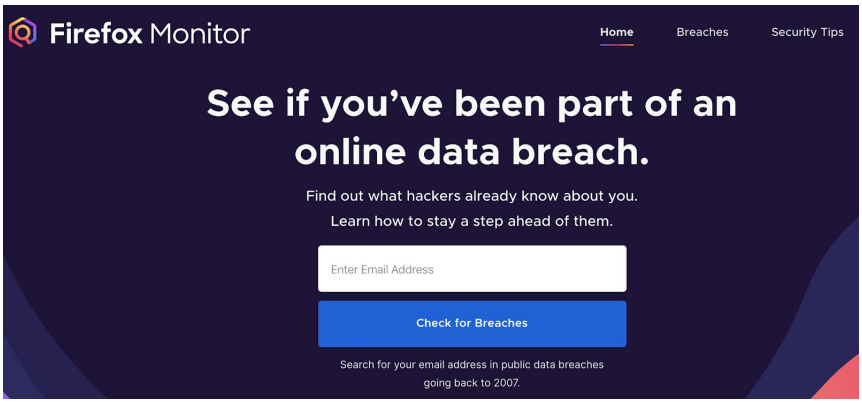
STEP 2: Checking your accounts

SLIDE 12 WORKBOOK 3

🕙 10 minutes

➔ There are tools online that share whether your account has been breached and what information was taken. Introduce participants to Firefox's Monitor tool.

➔ On a mobile device or computer, have individuals go to monitor.firefox.com and enter their email addresses.



Resource: Have You Been Breached?

Monitor.firefox.com is an online site that will tell individuals whether their data has been breached and what data is shared with third-party platforms or apps. The site also shares tips on how to secure your data after a breach and what information you should change. Just

because a platform or app has been breached doesn't mean someone shouldn't use it. Instead, consumers should ensure safety by changing their personal information.

- ➔ The result page shows that the accounts associated with that email address have been hacked and information has been shared or obtained without your permission. Each account listed says which of your information was obtained by hackers, and often includes your email, password, and IP address.
- ➔ Discuss the findings as a group using the following prompts and ask participants to reflect upon what they found. Remind participants to not share sensitive information or details that would make them uncomfortable at this time.

? Questions

- Raise your hand if your information was shared in a public breach.
- Were you aware your data had been breached?
- Does anyone want to share their reaction to their findings? How does it make you feel to learn your accounts have been breached?
- How many of these services do you recognize? Did you forget about any of the accounts that you see listed?
- Were your breached passwords used on other sites? When will you change those passwords?

STEP 3: How to create a strong password

 **SLIDES 13 and 14**

 **WORKBOOK 3**

🕘 10 minutes

- ➔ As a group discuss the importance of creating strong, unique passwords for each account.
- ➔ Brainstorm out loud a list of ways to create a strong password—write the list on paper, a board, a document, or a place where it is visible to everyone in the room. Once the ideas are exhausted, share any in the list below that were not mentioned.
- ➔ Using the list, ask participants to brainstorm a new password. After developing what they believe is a strong password, invite them to share it with the group. Then ask them to test it online at howsecureismypassword.net.

Resource: How Secure Is Your Password?

Howsecureismypassword.net is an online site that will tell individuals how strong their password is, as well as how long it will take a computer to solve for it. It will share tips on how to improve the password for future use.

➔ Ask participants to repeat the above exercise using new passwords until they come up with a password they believe is secure. As a group, discuss and assess the new passwords. Remind participants to not use these passwords after the workshop, but test and use new ones.

What Makes a Strong Password

- **A long password.** Use at least 8 to 12 characters.
- **Different passwords.** Have different passwords for different tools.
- **Mix of characters.** Use a variety of capital or lowercase letters, numbers, symbols, etc.
- **Nonpersonal.** Don't use passwords such as names, birthdays, family members, addresses, etc.
- **Not typical.** The top three passwords in 2018 are: 12345, password, 123456789.
- **Has phrases.** Add many words to the password. Don't hesitate to use spaces if you can.
- **It's complex.** Passwords don't always need to make sense.

Activity 2: How hackable is your security question?

SUMMARY:	Facilitators will discuss how to create strong passwords, security questions, and tools available.
OBJECTIVES:	➔ Understand how security questions can be uncovered. ➔ Know how to pick and answer security questions.
APPROX. TIME:	15 minutes
AUDIENCE:	Beginner level
ACTIVITY TYPE:	Individual quiz activity and group discussion
MATERIAL:	Pens

STEP 1: Security question test

 **SLIDES 15 and 16**

 **WORKBOOK 4, 5, and 6**

10 minutes

- ➔ Ask participants to complete the security question test in their workbook. Participants should pick one of the security questions to test, ideally one they have personally used or are familiar with.
- ➔ Come back as a group for a discussion using the prompts. Remind the group that they don't need to share their answers or any sensitive information.

? Security Questions

Security questions are meant to be easy to remember, but often they are about personal information that is easily accessible online—this test is meant to show that and have participants see the connection between what they share online and how someone can use that data.

? Sample Prompts

- How many people got “hacked”? How did that make you feel?
- Will you change or modify your answers online?
- Will you change your future questions or answers?

STEP 2: Practices for picking strong security questions

🕗 5 minutes

➔ As a group, discuss how to select a strong security question and a good answer.

Picking Strong Security Questions and Answers

- These questions should be easy for you to remember but hard for others to guess.
- Could have many possible answers (e.g., old cell-phone numbers).
- Is not easily searchable or known by other sites (e.g., anniversary dates or pet’s first name).
- Not listed on online profiles (e.g., city you were born in).
- Is not a physical item that can be easily found (e.g., car license plate).
- You can make up a fake answer (e.g., instead of mother’s maiden name put father’s first name).

Activity 3: Password management tools

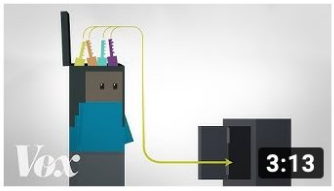
SUMMARY:	A discussion of password managers.
OBJECTIVES:	➔ Discuss and recommend available password management tools.
APPROX. TIME:	15 minutes
AUDIENCE:	Beginner level
ACTIVITY TYPE:	Group discussion
MATERIAL:	Video

STEP 1: How to secure your passwords

SLIDES 17, 18, and 19 **WORKBOOK 7 and 8**

5 minutes

➔ Remembering complex passwords can be hard. There are tools to help you manage your security online.
➔ Show the 3-minute VOX video below to understand how password management tools help secure your accounts.



Here's why you should stop memorizing your passwords
Vox
1.8M views

➔ After the video, follow the prompts.

? Video Prompts

- Does it make sense why we need password management tools?
- Would you secure your password in a tool after the workshop?
- Any questions on how password management works or why it is used?

STEP 2: Password management tools

🕘 5 minutes

➔ Discuss password management tools that participants may have used in the past or know.
➔ List the tools below and ways they help provide security. Write the names of tools somewhere visible.

Resource: Password Management Tools

- Password management tools allow us to store, generate, and track login passwords to the multiple services and platforms we use online. Those services/platforms are stored in the password management tool and can be accessed only by creating a strong, master password to log in. When you log in, the tool will retrieve those passwords and populate them in those services and platforms.
- Four of the most highly recommended and used password managers are Dashlane, KeePass, LastPass, and 1Password. These managers are cloud-based and live inside your browser as an extension.
- Some password managers offer a free version that is limited in features, such as LastPass. Some are cloud-based but can also be installed offline. That is the case with 1Password. Most of the password managers are available for major browsers, including Chrome, Firefox, Safari, and Opera.
- Major browsers also offer built-in password managers, such as Chrome's password manager, Firefox's password manager, and Safari's iCloud Keychain. These are easy to use and give added security.
- One downside to using a password manager is that if you forget your master password, you are locked out of the account forever. And you will need to reset each account that you stored in that manager individually.
- It is important to note that password managers can also be hacked but use encryption in their tools to help make sure your data is kept safe from breaches. Encryption is covered in the next module, but it is the process by which you, and only you, can enter your digital safe and ensure the privacy of passwords.

STEP 3: Two-factor authentication

🕘 5 minutes

➔ Discuss as a group the definition of two-factor authentication. It might have already come up in conversation, and individuals might already be using it. If so, ask them to explain what happens when they use it and why they have enabled it.
➔ Turn to the workbook to view steps on how to set up two-factor authentication.

Two-Factor Authentication

- Two-factor authentication is an additional layer of security on your digital accounts. After inputting your account info, such as username and password, two-factor authentication requires you to verify your login through a third-party app, email, or mobile device. This often looks like a text with a code you input on the site or an email with a verification link you click.
- You can set up two-factor authentication for online banking (PayPal), social media (Facebook), accounts (Google), or online stores (Amazon).

Conclusion

PAGE 20 OF PRESENTATION	
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 20 and 21**

5 minutes

 **WORKBOOK 9**

- ➔ If you are a small group, go around in a circle and have everyone comment on something they learned, found interesting, or will do differently as a result of the workshop.
- ➔ If you have a large group, ask individuals to break off into pairs and discuss their reflections with another person. Bring the group back together and ask whether 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 else who didn't attend this workshop?

STEP 2: Next steps

SLIDE 22

5 minutes

- ➔ Discuss what happens after the workshop. Is there another workshop happening? 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 review and install a password management tool. In a follow-up email, have them indicate which tool they chose.

Resources and Links

The resources and links below are to aid your workshop. That means 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: Tips for better passwords
https://www.consumerreports.org/digital-security/tips-for-better-passwords

ARTICLE: Everything you need to know about password managers
https://www.consumerreports.org/digital-security/everything-you-need-to-know-about-password-managers

ARTICLE: 773 million consumer accounts had email and passwords exposed
https://www.consumerreports.org/privacy/consumers-had-email-and-passwords-exposed

ARTICLE: The best way to use two-factor authentication
https://www.consumerreports.org/digital-security/best-way-to-use-two-factor-authentication

VIDEO: Why use password management tools
https://www.youtube.com/watch?v=xHSnHj-zKF4

Password Management Tools

- Dashlane: dashlane.com
- KeePass: keepass.info
- LastPass: lastpass.com
- 1Password: 1password.com
- Chrome's Password Manager: support.google.com/chrome/answer/95606
- Firefox's Password Manager: mozilla.org/firefox/features/password-manager
- Safari's iCloud Keychain: support.apple.com/HT204085