Cybersecurity 101:
Use MultiFactor Authentication

Curriculum Guide

Consumer Reports and Cybersecurity

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. Some of the most intimate aspects of our lives unfold through devices and online services. However, there are big questions about whether the devices and services we use respect our privacy, and whether they adequately safeguard our information. It is easy to feel overwhelmed by the challenge of staying safe online.

That's why Consumer Reports launched Security Planner. Security Planner is a free, easy-to-use guide to staying safer online. It provides personalized recommendations and expert advice on topics such as keeping social media accounts from being hacked, locking down devices ranging from smartphones to home security cameras, and reducing intrusive tracking by websites.

Our team of experts has worked on adapting content from Security Planner to create easy-to-use curriculum for any learning spaces. We're 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. We can't say this enough: Thank you for helping us create a more informed and safer world.

Introduction to the Curriculum Guide

We know that running a workshop can be hard. We also know that teaching cybersecurity 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 the basics of cybersecurity 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.

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 topic
OBJECTIVES:	➔ Introduce facilitator(s) and participants. ➔ Set ground rules.
ESTIMATED TIME:	10 minutes
ACTIVITY TYPE:	Group discussion

STEP 1: Introductions

🕐 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 cybersecurity 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 info on cybersecurity that we've gathered below.)*
- ➔ Review the agenda and share why the topic you chose is important—what are the threats and concerns we face because of it?

Why Cybersecurity and MFA?

- We are increasingly surrounded by new technologies, and though they are fun and convenient to use, the personal details we are sharing are often at risk.
- Criminals buy and sell information stolen in data breaches, including passwords. In addition, they can use software designed to cycle through huge dictionaries of common passwords. This means that a password alone might not be enough to protect you.
- 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.

STEP 2: Ground rules

🕐 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 and security, 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.

Multifactor Authentication

SUMMARY:	In this module, facilitators will learn types of MFA and how to set them up
OBJECTIVES:	➔ Understand what is MFA ➔ Discuss types of MFA ➔ Set up MFA on devices
APPROX. TIME:	30 minutes
MATERIAL:	Post-it Notes Pens Internet-connected devices (computers and smartphones)

Activity 1: Understanding MFA (5 mins)

STEP 1: Data Breaches

🕐 5 minutes

➔ Discuss as a group the term ‘data breach’ and ‘multifactor authentication’.

? Data Breaches

In 2021, over 22 billion records were part of a data breach. As this number increases it’s likely that most people’s information has been shared in a breach online.

Things to consider:

- Did you receive notification that your login and password are part of a breach?
- What actions did you do as a result?
- If your password was shared, what can you do to protect yourself?

Multifactor Authentication
MFA strengthens login security by requiring an additional piece of information beyond your password. If your password turns up in a data breach or if someone looks over your shoulder, your account is more secure because the person trying to access it will also need that second piece of information. It means that when you enter your login details, you have to enter or do an additional action to get into your accounts.

Activity 2: Types of MFA (15 mins)

STEP 1: SMS-based MFA

🕗 5 minutes

- ➔ Ask participants if they have ever received a text message to verify they logged into an account?
- ➔ Review the definition of a SMS-based MFA

Definition
Often, receiving codes via text message or email is the only option for some online services. This is the method familiar to most people. Any time you log into a digital account via a new laptop or smartphone, you're required to enter your password and then a multi-number code that gets texted to your phone.

STEP 2: Authentication App

🕗 5 minutes

- ➔ Review the definition of an Authentication App. Discuss how it’s different from a SMS-based MFA.

Definition
It is safer to set up MFA using an authentication app, such as Authy or Google Authenticator or Microsoft Authenticator or Duo. These apps are often recommended by security experts because codes sent by text message or email can sometimes be redirected or intercepted. When you need to verify yourself using MFA, you can open up the app and click to verify the account.

STEP 3: Security Key

🕐 5 minutes

➔ Review the definition of a Security Key. Discuss how it's different from a SMS-based MFA and Authentication App.

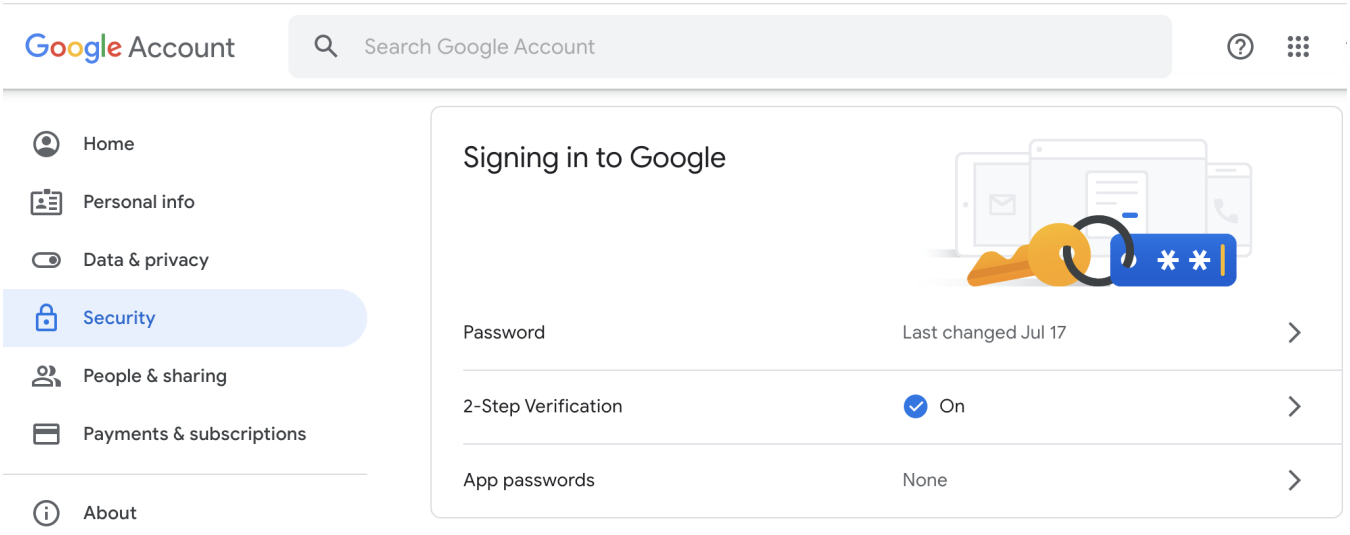
Definition
Security keys are another way to use multifactor authentication. They are small pieces of hardware, usually small enough to fit on a keychain. After you enter your password, you plug in your security key or tap it against your device, for wireless models. Unlike other methods of multi-factor authentication, security keys are phishing resistant. However, they do have three disadvantages: You have to buy them, you have to carry them around (or keep them plugged into your computer), and they aren't supported by every service that offers MFA.

Activity 3: Setting up MFA (10 mins)

STEP 1: Enable MFA on Google

🕐 5 minutes

➔ To set up MFA on your Google account, go to your Gmail inbox or any other Google page. Then click the grid icon in the top right and go to Settings. Click on Account (you may need to sign in first) > Security > Signing into Google > 2-Step Verification > Turn on.

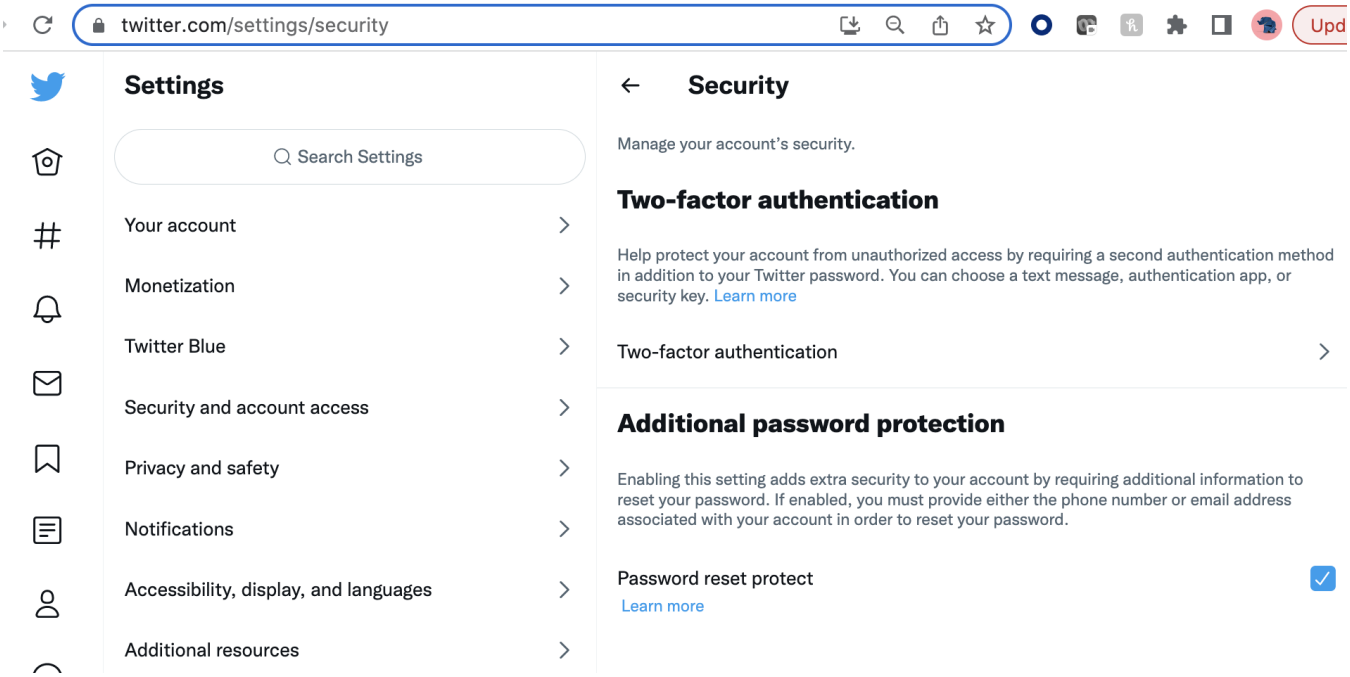


STEP 2: Enable MFA on Other Accounts

🕐 5 minutes

➔ Encourage participants to set up MFA on another account. MFA can often be turned on by clicking settings/preferences and following the security/privacy steps. Sample accounts include Social Media, Online Banking, Email, Shopping Accounts, Gaming Console, Smart Devices etc.

Example: Turning on MFA on Twitter



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:	5 minutes
ACTIVITY TYPE:	Group discussion

STEP 1: Final comments

🕐 5 minutes

- ➔ Facilitate a brief and reflective discussion about how to set-up MFA for participants online accounts.
- ➔ If you are 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 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 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 else who didn't attend this workshop?

Resources and links

The resources and links below are to aid your workshop. You can share them before, during, or afterwards with participants.

Additional Resources
ARTICLE: Set-up multifactor authentication https://securityplanner.consumerreports.org/tool/set-up-multifactor-authentication-mfa **ARTICLE:** Use a security key for stronger MFA https://securityplanner.consumerreports.org/tool/use-a-security-key-for-strongest-mfa **ARTICLE:** Protect your financial data https://securityplanner.consumerreports.org/tool/protect-your-financial-data **ARTICLE:** Secure your gaming console https://securityplanner.consumerreports.org/tool/secure-your-gaming-console