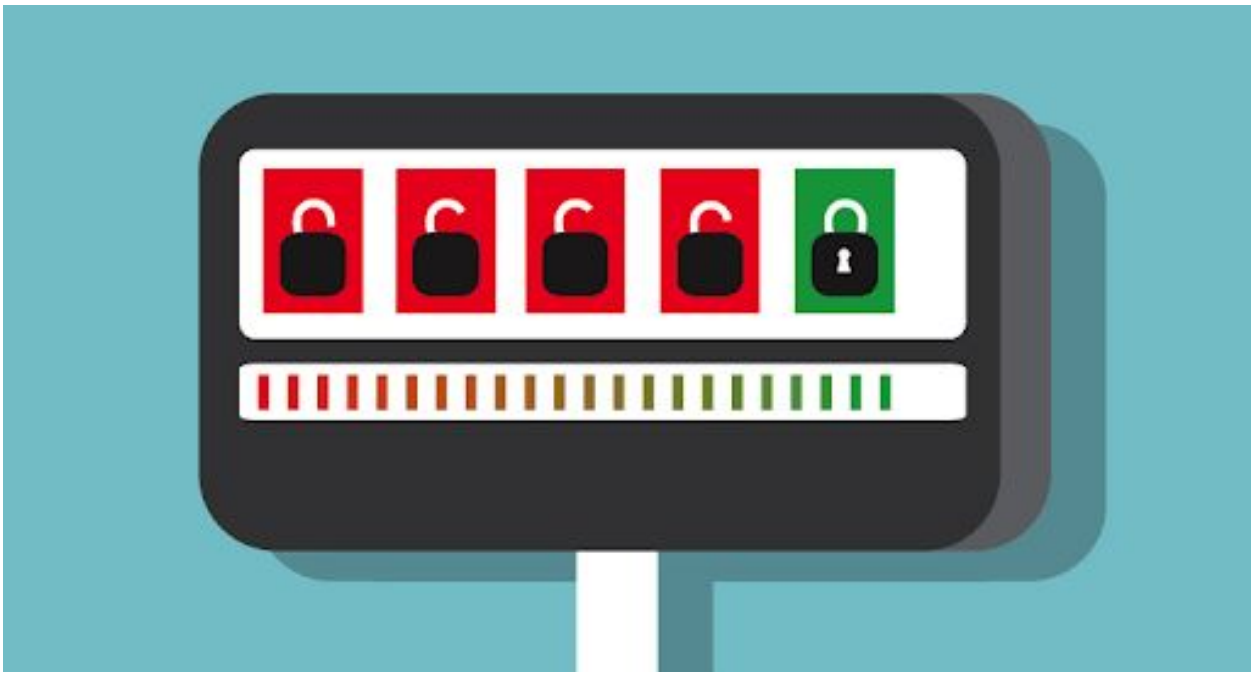

Protecting Your Online Privacy

Encryption and Phishing

Participant Workbook

V 1.3

Welcome and Introduction

What are the threats to our digital privacy?

Icebreaker (in Pairs)

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 do you find scary or unfair or strange about technology?

Additional Notes:

Activity 1: The Key to Encryption

Personal Information (Group)

What types of personal information do you share on the web?

Storing or sending sensitive information (group):

List ways you can relay sensitive information on the web.

- **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, which indicates that the connection is only partially protected.
- **See out sites with URLs that start with "https" (vs. "http").** The "s" stands for "secure," and this addition to the URL ensures that your communications with the site aren't seen by unknown third parties.
- **Use trusted platforms.** Leverage 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 misplaced or left unattended. Make sure the passwords are hard to guess; don't make them "0000" or "password."

Crack the Code Activity (Individual)

Complete the activities below. Can you solve for the hidden text or code?

What is the secret message?

Eceip fo ekac

Can you open this lock? What is the three-digit key?

HINTS:

5	6	1

One of these numbers is right and in the right order

3	9	4

One of these numbers is right and in the right order

2	6	7

One of these numbers is right and in the right order

1	7	5

Two of these numbers are right and in the wrong order

2	3	6

Nothing is right

Now it's your turn! Imagine you want to tell someone your favorite color but you didn't want others to know it. Create a secret code to describe your color. Examples of how to create a code include:

- Write the word backward.
- Go five spaces forward or backward in the alphabet when choosing which letter you want.
- Scramble the letters in a word.
- Create a number key that is assigned to letters of the alphabet.
- Make up a secret language, such as pig latin.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	2	3	4	5	6	7	8	9	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
14	15	16	17	18	19	20	21	22	23	24	25	26

Write your favorite color in code:

Share your code with someone near you. Can he or she guess your favorite color? Can you guess his or her favorite color?

Definition: Encryption

Encryption is the process by which you alter or change a message to hide its meaning. The message is changed so dramatically that it is unreadable unless you know how it was edited. Many online sites and tools use encryption to protect your data and information. For example, if your password is ‘test123’ it will be encrypted and appear as ‘635h7n3’ so that hackers or third parties are not able to view the text.

What are ways you encrypt your files or data?

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

Popular Encryption Tools (Group):

If you want to encrypt **one** file:

AxCrpt: axcrypt.net
7-Zip: 7-zip.org

If you want to encrypt **all** your files:

VeraCrypt: veracrypt.fr
BitLocker (available in Microsoft Windows versions)
FileVault 2 (available on Mac computers)

Messaging Apps:

Signal: signal.org
Viber: viber.com

Additional Notes:

Activity 2: Phishing

What Is Phishing (Group)?

Definition: Phishing

Phishing can be best defined as a scam that is meant to obtain an individual's sensitive information, such as passwords, credit card numbers, Social Security number, and more.

Case Study (Individual):

Taylor received an urgent email from his bank account asking for immediate action. Taylor isn't sure what to do and needs your help. Read the email and answer the following questions.

From: Trusted Bank <trustedbank@hotmail.com>
To: Taylor Good <taylorgood@gmail.com>
Subject: Immediate Action Required: Update Bank Information

Dear Valued Customer,

It has come to our attention that there has been a billing error associated with your account. Due to the error, we have suspended your account until reviewing the issue and proper verification has occurred.

To access and reactive your account, simply click the link below and follow the steps to enter your account details and password.

www.trustedbank.eg/activation

If completed within the next 48 hours, your account will resume as normal.

Thank you

Trust Bank Custumer Service Team
For customer service inquiries call 1-866-397-8541

What should Taylor do after reading the email? What steps should Taylor take to see if his bank account has been compromised?

Is this email real or fake? Create a list of the ways you know this email is real or fake.

How can you spot 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 have been scammed.

- If you are uncertain about whether you have 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 Federal Trade Commission at http://ftc.gov/complaint and the Anti-Phishing Working Group at reportphishing@apwg.org.
- Call appropriate companies, such as your bank and 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 it can alert other users.
- In some cases, you might have to download antivirus software on your computer.
- Enable multi factor authentication and encrypt your sensitive information.
- Change compromised information and passwords (if possible).

Conclusion

Final thoughts. What have you learned? What will you take away?

Make a commitment to helping the spam algorithms, and reporting five emails as spam (you can even look in your spam filter!). Set a date and time that you will review and install a password management tool.

Date:

Time:

Additional Notes:

Glossary of Terms

This is a list of terms that may come up during this workshop. You may or may not be familiar with them. Feel free to ask questions, but also refer to this glossary as a resource.

Big data are large datasets that are analyzed by sophisticated technology to determine patterns, trends, and association about human behavior, people, places, etc.

Cyberstalking is using the internet to stalk or harass an individual or group.

Data breaches are intentional or unintentional release of secure or private/confidential information to an untrusted environment.

Data brokers are people or companies who gather personal info and contact details of many people from a variety of sources and sell lists to their clients for advertising, and other targeting/personalization tasks.

Dataset is a collection of data/information about a particular situation or group of people that corresponds with some type of database in order to analyze patterns and variations.

Digital citizen is a person who develops the skills and knowledge to effectively use the Internet and other digital technology.

End-to-end encryption is a process of transferring information that only you and the intended recipient of that shared data or piece(s) of info can read or access. If someone else intercepts that data—including the intermediary that delivers the message—it will look like scrambled letters and numbers that don't make much sense.

Facial recognition is the process of uniquely identifying individuals based on facial features via software.

Firewalls monitor and control the traffic flow of information to and from a local computer network and act as a defense system for that network from attacks and malware.

Hacking is an act or a series of actions to manipulate hardware or software to get access to information, machines, or resources in a way that it was not originally intended.

Internet protocol (IP) address refers to a unique set of numbers that is assigned to each device connected to the internet so that devices can find and speak to one another. An IP address can expose information about the user's internet connection and location.

Internet of Things (IoT) refers to a list of devices that connect to the internet, beyond just computers and smartphones, which can be monitored or controlled from remote locations.

Malware is short for malicious software and comes in many forms. Code that is designed to

control, disable, and steal resources from a user's computer, such as passwords, financial information, and more.

Metadata is data about data. There are many forms of metadata, for example the title and artist of an mp3 rather than the music itself. A useful analogy would be the information displayed on the outside of a sealed envelope. It contains who sent it and from where, not the letter content.

Multifactor authentication (MFA) is a security feature that requires information beyond a password and username to verify a user's identity before log-in can be authorized. These methods include SMS, authenticator apps like Google Authenticator or a USB key.

Online surveillance is the monitoring of an individual's computer, technology devices, and online activity to understand their behavior, view their information, and watch their activities.

Peer-to-peer (computing or networking) is a decentralized system of individuals/users sharing data without a third party or centralized server.

Pharming is a type of cyber attack in which users input a web address but are redirected to an unsecure or fraudulent website without the user knowing.

Phishing is a type of social engineering in which an attacker pretends to be a legitimate and credible authority in order to get people to unwittingly provide information such as passwords, credit card numbers, or wire transfer info.

Privacy by default prioritizes the user's privacy by using default settings that provide maximum privacy without the user's intervention.

Social engineering is a technique to gather information or persuade someone into doing something outside of what should be expected or allowed. It often manifests as content on webpages, email, or advertisements that trick you into sharing sensitive personal information.

Spear phishing is a type of phishing that has a specific target. Hackers pretend to be people and/or businesses that a user knows in order to trick the user into downloading or clicking on a link in order to install malware.

Spyware is software that enables a user to obtain private information about another person's computer or its user.

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 log-in through a third-party app, an email, or a mobile device.

Virtual private network (VPN) is a tool that ensures your connection to the internet is encrypted. Some (most) VPNs also provide location masking by providing a false IP address to the website or server you connect to.

Volunteer Interest

Would you be interested in presenting a workshop similar to this one in your community, to your family and/or your friends, if given training and CR staff guidance?

☐ YES ☐ NO

If you answered **YES,** please fill out your contact information below, so someone from CR can follow up with you.

Name	
Phone Number	
Email Address	

Your Free Gift

As a thank-you for attending today's workshop, Consumer Reports is automatically giving you a three-month free **Digital Membership,** which includes digital access to our ratings and reviews (a $35/year value)! If you would **also** like to receive a free three-month subscription to the **magazine,** please legibly print your contact information below:

Name	
Phone Number	
Address	
City, State, ZIP	
Email Address	

DON'T WANT YOUR FREE GIFT?

☐ I **DO NOT** wish to receive my FREE gift. (Please write your name below to ensure that we take you off the list to receive a free gift.)

Name: _____

Email Address: _____