SECURITY AND PRIVACY

INTRODUCTION

You can do a lot to protect your accounts from theft and keep your personal activities secure online. Depending on where you live, the work you do, or other issues, you might have reason for concern about your safety **engaging with digital information and tools**. You might also have concerns about the **safety of the people you communicate with**. Digital privacy and security practices cover a broad range of activities but in the following you will learn how to better protect yourself with a few essential habits and tools. Activities that we use our computers, phones, or other digital devices for generate data. Even when we feel that we are doing something on our own, **third-parties frequently access and track this data**. We know when we enter personal information to sign-up for a new app, but it's frequently less obvious how that app or a web browser permits other parties to access the data produced during use. Some data, such as a phone number could identify us while other data, such as the city our internet connection is in, might not. Nevertheless, enough data collected can sometimes permit another party to identify us. That other party could have criminal intent, it could be an authoritarian government, or it could be something benign. However, regardless of how benign it might appear, that third-party now has data that if misused or used in unexpected ways in the future will jeopardize our well-being.

RISKY PRACTICE ONLINE

You might forego some privacy in exchange for being able to use a particular service or application but be cautious, it's easy to get into online behaviours that risk your privacy and security. Here are five risky behaviours to be aware of:

1. Interacting with insecure websites. For example, indicators appear in the address bar of browsers like Firefox and Chrome , which tell you about the security of the site you're currently browsing.
2. Permitting your web browser to expose more data than is necessary. Default settings might permit other sites to place or access cookies inappropriately and track your online activities (see the Data Detox Digest).

3. Allowing your social media profile information to be accessible to people or services that you do not know or trust.
4. Installing software from a dubious source (it might turn out to be malicious).
5. Registering for online services without awareness of their background.

Ask yourself questions such as:

- Is this site using secure protocols or other technologies?
- Have I reviewed the default settings of the applications I'm using?
- What does the organization providing the service I'm about to use do with user data? What sort of accountability can I expect?
- Is the organization or source a commercial entity, individual, non-profit, government, or some other entity? Motivations vary.
- What jurisdiction does the organization operate under and where does it store its data?
- How comfortable am I trusting the source this software or service comes from?

Source: screenshot of Data Detox Browser Digest by Tactical Tech is licensed as CC BY-NC-ND 4.0

WHAT WILL COMPROMISE YOUR SECURITY

A person's digital security can be compromised via technical means but also frequently in the form of simple tricks that rely on trust or lack of awareness. Those tricks are often referred to as **phishing**. An example of phishing would be receiving an e-mail message from a source that looks familiar

and includes a link to click. If you do not check the underlying e-mail address that sent the message or do not check where the link goes before clicking it, you may unwittingly provide information to a malicious party.

Your devices can be infiltrated through the installation of insecure applications even if they appear harmless. Sometimes opening a file attached to a message can result in the installation of a **malicious program**. Permitting an application to access unnecessary features on your device can enable a third-party to gain access where it shouldn't have it. This guide on malware provides techniques to protect your computer and mobile devices against these sorts of attacks.


THE 7
RED FLAGS
OF PHISHING
Phishing is one of the most common threats you can encounter online. Luckily, phishing messages can be easy to spot – if you know what you're looking for.
Here are the 7 biggest red flags you should check for when you receive an email or text.
1
URGENT OR THREATENING LANGUAGE
Real emergencies don't happen over email.
LOOK OUT FOR:
Pressure to respond quickly
Threats of closing your account or taking legal action
2
REQUESTS FOR SENSITIVE INFORMATION
Anyone asking for personal information over email or text probably shouldn't be trusted with it, anyway.
LOOK OUT FOR:
Links directing you to login pages
Requests to update your account information
Demands for your financial information, even from your bank
3

Source: screenshot of "The 7 red flags of phishing" from Get Cyber Safe by Communications Security Establishment, Government of Canada.

Text version:

Phishing is one of the most common threats you can encounter online. Luckily, phishing messages can be easy to spot – if you know what you're looking for.

Here are the 7 biggest red flags you should check for when you receive an email or text.

1 Urgent or threatening language

Real emergencies don't happen over email.

Look out for:

- Pressure to respond quickly
- Threats of closing your account or taking legal action

2 Requests for sensitive information

Anyone asking for personal information over email or text probably shouldn't be trusted with it, anyway.

Look out for:

- Links directing you to login pages
- Requests to update your account information
- Demands for your financial information, even from your bank.

3 Anything too good to be true

Winning a lottery is unlikely. Winning a lottery you didn't enter is **impossible!**

Look out for:

- Winnings from contests you've never entered

- Prizes you have to pay to receive
- Inheritance from long-lost relatives

4 Unexpected emails

Except the unexpected, and then send it right to the **trash.**

Look out for:

- Receipts for items you didn't purchase
- Updates on deliveries for things you didn't order

5 Information mismatches

Searching for clues in phishing email puts your love of true crime podcasts to good use.

Look out for:

- Incorrect (but maybe similar) sender email addresses
- Links that don't go to official websites
- Spelling or grammar errors, beyond the odd typo, that a legitimate organization wouldn't miss

6 Suspicious attachments

Attachments might seem like gifts for your inbox. But just like real gifts, they're not always good…

Look out for:

- Attachments you didn't ask for
- Weird file names
- Uncommon file types

7 Unprofessional design

For some reason, hiring a graphic designer isn’t on a cyber criminal's priority list.

Look out for:

- Incorrect or blurry logos
- Company emails with little, poor or no formatting
- Image-only emails (no highlightable text)

If you spot any of these red flags in a message:

- don’t click any links
- don’t reply or forward
- don’t open attachments

Delete the **email or text**, or reach out to the sender through a different channel if you're not sure.

Get more tips to protect yourself and your devices at: GetCyberSafe.ca

FIVE ROUTINES FOR PRIVACY AND SECURITY

Changing your habits and using privacy-oriented tools reduces what other parties can access about your activities. Implement the following routines to improve your online privacy and security.

1. Make your information unreadable by **encrypting** it. Only those permitted can make it readable again (decrypting often involves a password and an application). You can encrypt documents on your computer or data that you are transmitting. For example, check that your web browser shows “**https**” rather than “http” in the address bar.
2. Use a **password manager** (e.g. BitWarden or KeePassXC) to securely store and generate passwords. Enable **multi-factor authentication** to decrease the likelihood of unauthorized access to your accounts. Learn how from this guide for creating and maintaining strong passwords.
3. Have a **secure file backup strategy** in the event that a malicious party gains control of your computer. Using an automated cloud backup service should include a no-knowledge/zero-access assurance that even the provider cannot read your information (see

this guide for backing up and recovering information).

4. **Switch to secure services** for messaging, e-mail, and office productivity types of tools. Examples include Signal, Proton Mail, and CryptPad. See more examples from PrivacyTools.io.
5. Connecting to a **virtual private network** (e.g. ProtonVPN or Mozilla VPN) conceals your true Internet connection from surveillance and provides other security benefits. Discover how VPNs work from the Center for Democracy & Technology. This article will help you choose a VPN.

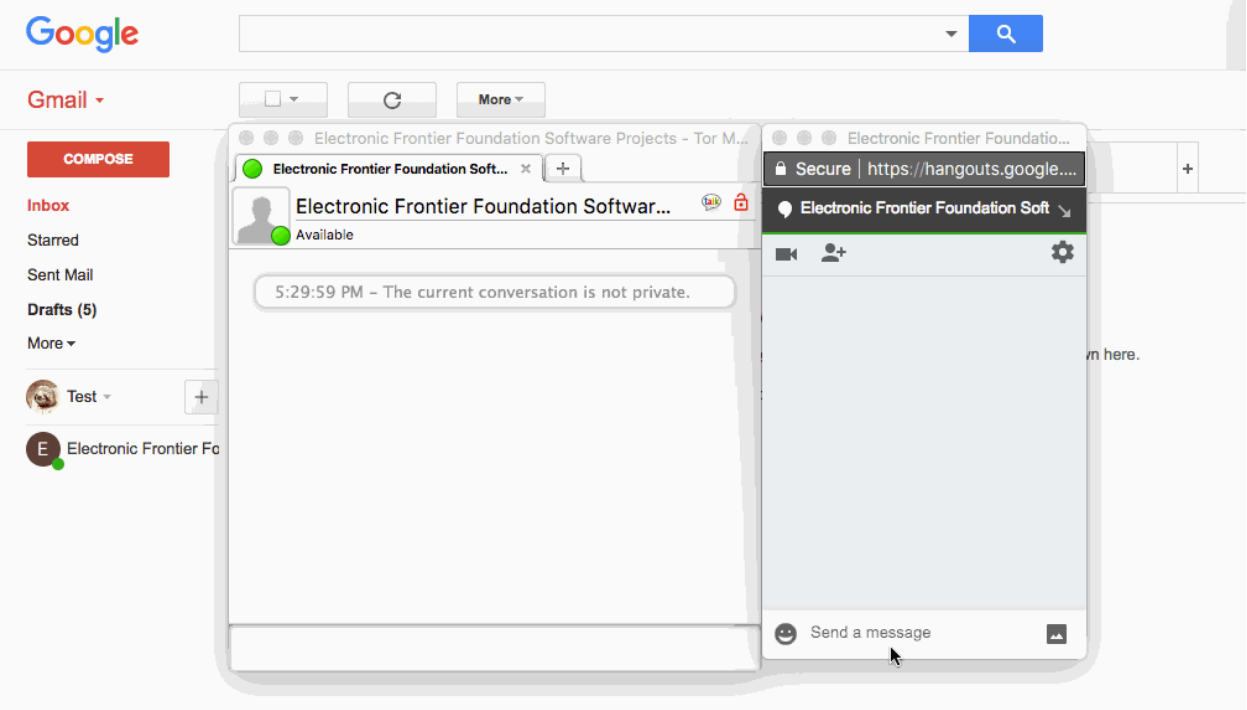

Image description: gif illustration from Electronic Frontier Foundation Software https://sec.eff.org/uploads/upload/file/23/OTR-Client.gif

CONCLUSION

New techniques regularly emerge for encroaching on people's online privacy. It won't be possible to perfectly secure all your digital activities on your mobile devices and computers. However, you can decrease the likelihood that you will have to deal with the consequences of having your personal data exposed. Continue to evaluate the services and applications you use while also taking

advantage of new, more secure routines.

We recommend the following resources for shoring up your privacy and security online.

1. The Data Detox Kit is especially useful for your mobile devices and social media presence.
2. Zebra Crossing is an easy-to-use checklist that covers the issues raised in this guide and many more.
3. Security-in-a-Box is a long-running site of resources, explanations, tips, and approaches to digital security.
4. The Electronic Frontier Foundation's Surveillance Self-Defense site provides many guides on specific types of security tools.
5. Concordia's FAQ on protecting your identity and other security advice.

ACTIVITY

Purpose: This activity will help you become aware of and reduce the information that you currently expose online.

Tasks:

1. Try the Cover Your Tracks test. This tool reveals what your browser currently permits other parties to know about your online activities. It also recommends changes that you can make to your settings. Test your changes with different sites that you frequently use; you may see warnings about what the site can or cannot do.
2. Verify your account and profile settings on social media or other sites that you frequently use. Explore how to limit the data stored about your app use. Follow the Data Detox Kit for social media profiles, which will help you understand how your profile data can be used and how to adjust your settings for more privacy.

Time: This activity should take about 15 minutes to complete.

ACTIVITY

Purpose: Gain know-how to analyze phishing scams.

Tasks:

1. Recognize things that should raise your suspicions from this infographic on the 7 red flags

of phishing.

2. Browse the Canadian Anti-Fraud Centre's examples of common phishing-style scams. Can you identify some of the red flags of phishing in these examples?

Time: This activity should take about 10 minutes to complete.

ACTIVITY

Purpose: You will see encryption in action and then try using an online service where encryption is enabled by default. Finally, get a start in securing your account login processes.

Tasks:

1. Watch this short animation of people using a Google chat tool before and after enabling encryption. Source:Transport-Layer Encryption vs End-to-End Encryption GIF by the Electronic Frontier Foundation.

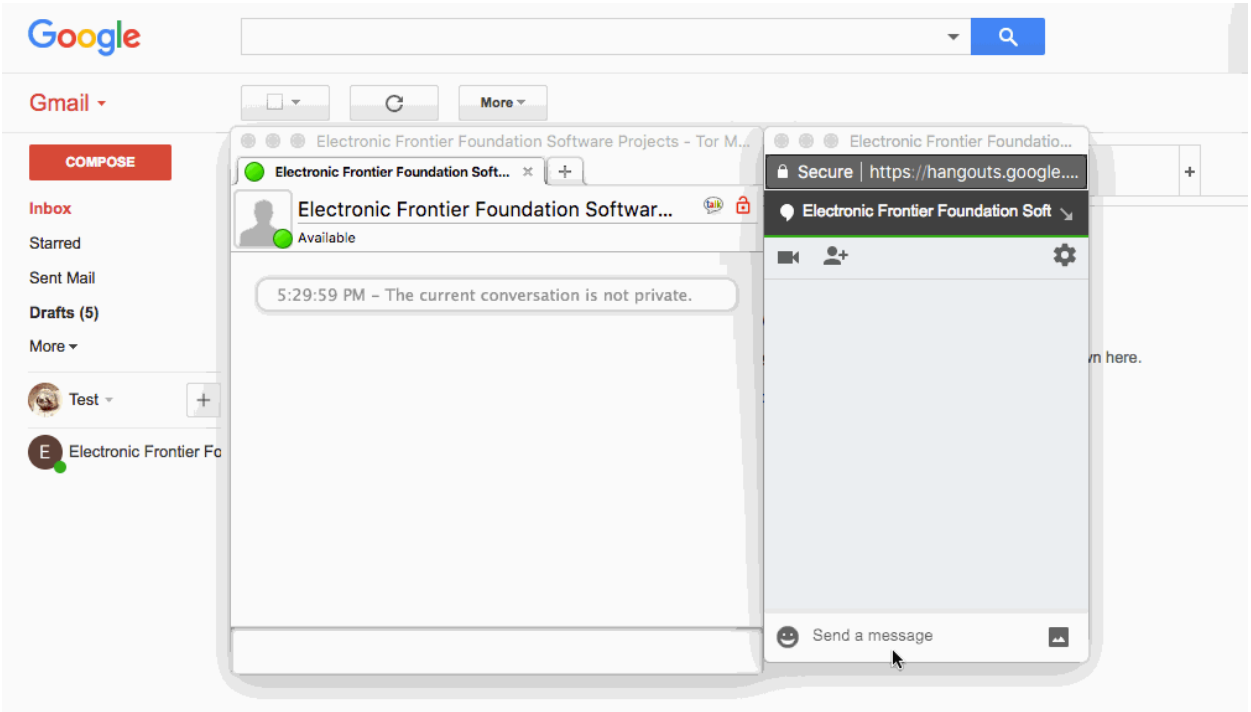

Image description: gif illustration from Electronic Frontier Foundation Software https://sec.eff.org/uploads/upload/file/23/OTR-Client.gif

2. Create a free account on CryptPad and familiarize yourself with its word processor; compare with Google Docs.

3. List the three services or applications you most frequently use. Explore your account or profile settings in each and look for terms like MFA or 2FA (two factor authentication) to determine whether they support multi-factor authentication. Follow the instructions in one to enable it and see how it works.

Time: This activity should take about 15 to 20 minutes to complete.

REFLECTION

Let's reflect on digital privacy and security. Read this article on Seven Steps to Digital Security. Think about these steps in relation to your current practices.

Write a short reflection (150-200 words) on how these steps relate to or may alter your current practices.

Time: This reflection should take about 15-20 minutes to complete.

FURTHER RESOURCES

Udemy course: The Ultimate Dark Web, Anonymity, Privacy & Security Course

Udemy course on how to access and use the internet privately, anonymously and securely

Video: What you need to know about stalkerware

A TED talk on software that is created to gain access to people's devices without their knowledge.

Webpage: The data detox kit

Information about how online services store and use your data and steps to follow for maintaining privacy and security.

REFERENCES

Get Cyber Safe. *The 7 Red Flags of Phishing*. Government of Canada 2020.

Front Line Defenders. *Backup and Recover From Information Loss*. 2021.

Electronic Frontier Foundation. Choosing the VPN That's Right for You. *Surveillance Self-Defense* 2019.

Electronic Frontier Foundation. *Cover Your Tracks*. 2022.

Electronic Frontier Foundation.Security Education Companion Glossary. *Security Education Companion.*

Front Line Defenders. *Create and Maintain Strong Passwords*. 2021.

Electronic Frontier Foundation. Seven Steps To Digital Security. *Security Education Companion* 2019.

Front Line Defeners. *Protect against Malware*. 2021.

Front Line Defenders. *Security-in-a-box: Related tools*. 2022.

Canadian Centre for Cyber Security. *Cyber Security Glossary*. Government of Canada 2022.

Canadian Anti-Fraud Centre. *Scams by Medium*. Government of Canada 2022

Jerome, J. Techsplanations: Part 5, Virtual Private Networks. *Centre for Democracy & Technology* 2018 October 16.

Data Detox Kit. Fortify Your Browser to Reduce Your Traces. *Tactical Tech* 2020.

Data Detox Kit. Renovate Your Social Media Profile. *Tactical Tech* 2020.

VIDEO TRANSCRIPT

Things for Digital Knowledge. Concordia Library.

Joshua Chalifour, Digital Scholarship Librarian

Intro slide: Concordia Library logo

Interviewer: there are a lot of issues related to online security and privacy. Can you tell me the risk that I have when I get online? [question displayed on the screen]

Joshua Chalifour: Yeah. You have a number of different ways that you're transferring information, which may be intentional, or it might be unintentional. And so, when you're using a web browser, for example, you transfer this information to a website. It can store something like a cookie in your browser, which has little bits of information in it that potentially other sites could access.

Visual: screenshot of Microsoft Edge browser setting on privacy

Joshua Chalifour: So, you want to be aware of what the default settings are in your web browser and determine how much of that you want to allow.

Visual image description: social media icons, comments, likes, etc.

Visual: video clip shows buttons that allow users to sign up for a service using their Facebook account, with the words “Continue with Facebook”

Joshua Chalifour: Other things like your social media profile, where you put a lot of personal information and make it accessible to other people. You know, sometimes you can use that to log in to another website and it can get access to some of that information as well. So, you want to be careful about who you're permitting to have access, and how much of that information you're getting in.

Visual slide text: risks associated with online activities: insecure website, too much permission, suspicious software, signing for up unknown service

Joshua Chalifour: There are other things like when you install software. And of course, you want to be careful about the source, where it's coming from, the apps and what the intentions are that they might have around providing that information to you.

Interviewer: How could this risky behavior compromise my security? [question displayed on the screen]

Joshua Chalifour: Well, there's a few different ways. So, I just mentioned software. Of course, if you install some software on your computer and it has malicious code in it, that might permit somebody else to have access to your files, for example. But the information that we are providing, if somebody gets access to it, allows them to trick you into doing certain things. And so, for example, you hear a lot about phishing in the news.

Visual: video clip shows hands doing screen touching movement.

Visual image description: a fishing hook is connected to a credit card.

Joshua Chalifour: And, you know, this is a case where you might receive an email from somebody and it may look trustworthy to you if you're not necessarily paying close attention to it and you click on a link and it will bring you to a website that maybe looks like your bank. And so, what they're trying to do is trick you into giving them information, perhaps about your financial accounts. And so, this is something that you would want to be cautious of.

Interviewer: That sounds dangerous. What should I do to protect my information security? [question displayed on the screen]

Joshua Chalifour: I would say it's a good idea to always reflect on the information you're providing and ask yourself some questions. So, you want to look at the sources of what you're working with here, whether it's a software application where it's being provided from, or let's suppose it's an online service that you signed up for.

Visual slide text: ask before acting: do I trust the sources of this software, is this site secure? What will they do with my data? Is this a private organization?

Joshua Chalifour: It's a good idea to ask, who is this organization? What kinds of policies do they have in place about how they store your data? And, you know, are they within some kind of legislation that would require them to take certain precautions? And if you get a good sense of what these organizations are doing, then you might make a determination that it's okay to trust them.

Interviewer: Sounds better. Can you give me some final tips on how to protect my information? [question displayed on the screen]

Joshua Chalifour: Yeah, I think there's a number of habits that you can put in place or routines that you might change. One of those, for example, would be around passwords. If you use the same password over and over on different sites and somebody gets access to it, of course, that opens you up to two problems in all of these sites.

Visual: a video clips shows encrypted password being typed in.

Visual: video clip shows the interface of a password manager.

Joshua Chalifour: So, if you use something like a password manager such as KeePassXC or BitWarden, this will help you generate passwords for different sites and keep track of them in a secure way. And so that can reduce that kind of risk. There are other things that you might want to do when you reflect on the types of online services that you're using, for example, is supposed to use a word processor to collaborate with other people. And there are some that will provide that same type of a service, but they will encrypt the information. So, what you're using doesn't stand as much of a risk of being accessed by somebody else. When you install software, of course you want to be careful about the sources we mentioned, but there are some other things that increasingly people will use virtual private networks.

Visual image description: two phones being connected by VPN.

Visual image description: a phone screen shows a green shield with VPN on it.

Joshua Chalifour: So, a VPN, this can help protect you against surveillance. When you're using the VPN, it makes it appear as if you're connecting to the Internet from somewhere else than where you actually are. And frequently they use encryption so that the information you're transferring will be more difficult for somebody to read.

Visual slide text: shows steps to navigate online security password manager, VPN, could back up, encrypting.

Joshua Chalifour: You might also consider having a backup strategy. So, in case somebody does get access to your files, at least you can restore them. And one of the ways that you might do that is to look into things like secure cloud backup services, which are just automatically backing up your files in the background. If you do something like that, it would be important to verify that they are zero access so that even the company themselves cannot access the files that you're that you're backing up. And you can do that on your own computer as well. Most computers now will allow you to encrypt the file system, or you can install programs to help you do that. So, these are some of the routines that you can develop to help you.

Visual: thank you and credit. CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon and infographics & images by Freepik. Music: Lofi Summer Background by Vladislav Kurnikov on Pixabay.