Tips for a Secure Email Account

A Note on Language

In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

An email address is more than just another method for someone to contact you. An email address is essential for most transactions these days, from activating a smartphone to making online purchases to setting up an online account. Your email account may contain sensitive and important communication and is often connected to important accounts, such as your bank. Ensuring that your email address is secure – that only you have access to it – is critical.

This tip sheet offers suggestions on how to make your email address as secure as possible.

Which Email Service to Choose

If you are worried about someone hacking your email (via man-in-the-middle attacks), an end-to-end encrypted email service may be what you want. For example, ProtonMail is completely encrypted and you can set it up so that the email is no longer available after a certain time. Other free encrypted email services include Tutanota and Mailfence.

Keep in mind, however, that these services may be slightly more complicated to use than traditional email. For example, some encrypted email services may require that the person to whom you're sending the email also uses the same email service or that to read the email, they click a link and read the email on a web browser. Keep in mind that encrypted email will not prevent someone from seeing your email if they know your email address and password or if you are using a monitored device.

It is possible to use a popular commercial email service, such as Gmail or Yahoo, and still have a secure account. Email security often comes down to passwords, the security of the device used to access email, and good email security and privacy habits such as those covered in the rest of this document.

Setting Up an Email Address

Email privacy and security start when you first create the email account.

Use Non-Identifying Information

Survivors of abuse and stalking may not want an email address that easily identifies them. When you set up an email address with a commercial email service, your email address doesn't have to use identifiable information like your name. You can use anything for your email address, such as *brightredstar3@gmail.com*.

During the setup, the email service provider will ask for information to associate with your email address, including your name and date of birth. You can use a pseudonym and a fake date of birth.

Just remember the pseudonym and birthdate you use in case you need that information to verify your account. Some email services also ask for your gender, mobile number, and a secondary email address. Some services allow you to bypass those questions without entering anything; this will vary according to the email service. For example, Gmail requires a name, username, password, date of birth, and gender; however, you can leave the mobile number and current email address blank and continue. Yahoo Mail requires a name, email address, date of birth, and mobile number while gender is optional. Outlook Mail only requires your name, email address, and password.

Use a Password No One Else Knows

For most people, the security of their email account comes down to whether anyone else knows their email address and password. Don't use a password that someone else can guess or a password that you also use for other accounts. Create a unique password that you can remember without having to write it down and is either a long phrase or contains letters, numbers, and characters.

Use Two-Step Verification

If you have a second email address or a secure mobile number (i.e. no one else has access to it), you can set up two-step verification. If someone tries to log in to your email account from another device or location, the email service will send a code to the second email or mobile number. The code will be required to sign in to the email account, in addition to the password. If you (or the person trying to log in to your email account) don't have access to that secondary email or mobile number to view the code, you can't sign into your account.

This is useful only if you have a secondary email or mobile number that no one else has access to.

If someone else does have access to that email/mobile phone, they could sign in to your account even with two-step verification, or it may let them know when you try to sign in to your account from a new location or device. Depending on your situation, you may not want to have two-step verification turned on until you first secure the secondary email and mobile number.

If you don't provide a secondary email or mobile number, the email service may periodically ask that you provide one when you sign in to your email account later on. In most cases, you can ignore these requests and hit continue or OK without entering anything. Secondary email and mobile numbers can be a very useful security step – but only if it works

for you. If you don't have a secondary email or mobile number, or the email or mobile number you have has been compromised by someone else, entering this information will not make your account more secure.

Make sure your secondary email account and mobile number are secure before you use either.

Review Security Notifications

Some email services will notify you of any security events in your account – such as changing your password, logging in from a different location or device, or changing any other security settings.

The security notifications may be sent to your secondary email address. Similar to the issue with two-step verification, if someone else has access to that secondary email address, they will know whenever you make any security changes to your account. You can choose to limit the notifications you receive or change the secondary email address to one that is more secure. (You can generally find the security notifications in the Security Settings section of your email account.)

Practice Good Email Habits

In addition to having a strong password and using the security features (e.g. two-step verification) the email service provides, practicing good email security and privacy habits is important to ensure that no one else can sign in to your email account or read your email.

Use Secure Devices

Try not to log in to your account on devices (e.g. mobile phones, tablets, computers) that the perpetrator has access to or is monitoring. Depending on how the device is being monitored, the person monitoring it may be able to see your email address and password if you log in on that device.

Always Log Out

Whenever you log in to your email account, whether it is on your own device or someone else's, always log out or sign off. Don't just close the web browser or app or shut down the device, as that will not log you off. If you don't log off, anyone who uses the device after you will be able to see your email account. Even on your own devices, logging off is helpful in case someone picks up your phone or computer or you lose it.

If you check your email on your mobile phone via the email app or on your computer/laptop via an email program, you may not be able to easily log off. In this case, you have a few options. Putting a passcode or password on the device will help limit this access. In some cases, you may even want to remove the email account from your email app or program. Some people do this when they are travelling or are concerned that someone untrustworthy could have access to their device. You can always check your email via the web browser or configure the email app or program to access your email after you are sure that your phone or computer is secure.

Don't Allow Your Browser or Mobile Phone to Remember Your Email Account or Passwords

Some email services (Gmail, in particular) have an option where the web browser will remember your account unless you tell it not to. The next time you (or anyone else) open the email sign-in page, your email address will be listed and all that is required is for someone to enter the password. Don't allow the web browser to remember your email account, particularly on devices that you don't own. This permission request will often show up as "Do you trust this browser?" Choose "no."

Some web browsers and mobile phones will ask if you want it to store your email passwords or to "remember me." In this case, it will remember both your email account and password. If you are concerned that someone else may have access to your devices, don't allow them to store your passwords. This may be convenient for some less sensitive accounts, such as your Netflix log-in, but you want your email account to be secure.

- **Don't Click on Links from Unknown or Suspicious Individuals**

For further security of your account and device, don't click on links from unknown or suspicious individuals or provide personal information via email or an email link.

- **Don't Send Personal Information through Email**

If someone (even if it's your bank or utilities company) is requesting personal information (such as passwords, credit card information, and bank information) via email, don't email back with the information. Instead, find the phone number for the company and call them back with that information.

Be Cautious When Giving Out Your Email Address

Since email addresses are what people use to contact you, you will need to give them to people.

However, you may not want to give out your email address to everyone who asks, particularly to stores or when setting up unimportant online accounts. Below are a few ways to provide an email address without having to give out your primary email address.

- You can create a junk email account for when you have to provide an email address but don't really want to receive emails from them. This email account is specifically for junk mail and should not be set up to receive important information such as statements from your bank, or be connected to important accounts, such as your mobile phone service.

- Some email services let you create short-term email accounts. These email addresses last 10 minutes to 24 hours, so they're very temporary. When you give out that email address, the emails are sent to that particular email service's website where you can check for the sent email. This is helpful for when you need to provide an email address to "confirm" signing up, but you don't want to provide your actual email address. Keep in mind that some of the temporary email services have no privacy, which means that anyone who knows the fake email address can see all the emails sent to that fake email address (examples of public temporary email services: Mailinator or Maildrop). Other temporary email services include Guerrilla Mail or 10-Minute Mail.

- A more long-term solution to protecting your email address is a service like Abine Blur. Abine Blur is a web browser extension for desktop and mobile that acts as a forwarding service. It "blurs" your real information so the receiver gets an anonymized email address, and not your actual email address. When they reply, Abine Blur forwards the

reply back to you to your real email address. On your end, you're sending emails back and forth like normal, but on the receiver's end, they only see the anonymized email address.

[RW1]Link 1.24

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support.

Adapted for Canada with permission from NNEDV's Safety Net project, based on their resource Tips for a Secure Email Account.

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

Women and Gender Equality Canada | Femmes et Égalité des genres Canada | Canada