BC Society of Transition Houses

Tips for a Secure Email Account

An email address is essential for most transactions these days, from activating a smartphone, to making online purchases, to setting up an online account. An email address is more than just another method for someone to contact you. 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 document offers suggestions on how you can make your email address as secure as possible.

WHICH EMAIL SERVICE TO CHOOSE?

Major email providers will let you set up as many email addresses as you want, for free. Some of these email providers include: Gmail, YahooMail, or Microsoft Outlook (formerly Hotmail). The benefit of these email services is that they are fairly easy to use. You can access them online via a web browser or set it up so that email is accessed via a mobile email app or computer email program.

If you are worried about someone hacking your email, an end-to- end encrypted email service may be what you want. There are email providers that offer email encryption. For example, ProtonMail is completely encrypted, and you can set it so that the email is no longer available after a certain time period. 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 service may require that the person to whom you're sending the email also use the same email service or that to read the email, they click a link and read the email on a web browser. Also 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.

Other ways in which you may have an email address is when you activate certain services, such as a broadband or DSL/ADSL (internet) service or when you create an apple ID (e.g., youremail@bigpond.com or youremail@icloud.com). Your school or your employer may also create an email address for you. Generally, these email accounts are automatically created and limited to your association with the school, employer, or service.

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.

BC Society of Transition Houses

SETTING UP AN EMAIL ADDRESS

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

- **Use non-identifying information**
  Women experiencing violence and stalking may not want an email address that easily identifies them. When you set up an email address with a commercial email service, the email doesn't have to be identifiable to you. You can use anything for your email address, such as brightredstar84@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 (and some require) your gender, mobile number, and a secondary email address. Some services allow you to bypass those questions without entering anything; if it requires the information, it will not let you complete setting up the email until you do. 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 someone knowing 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 password that is unique, 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 more than one email address or a mobile number – and it is secure (no one else has access to it) – you can set up two-step verification. If someone tries to log into your email account from another device or location, the email service will send a code to the second email or mobile number, which will be required (in addition to the password) to sign into the email account. If you (or the person trying to log into your email account) don't have access to that secondary email or mobile number, 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/smartphone, they could sign into your account even with two-step verification or it may let them know when you try to sign into 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 into 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 and 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 is secure before you use it.

- **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 had 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 (two-step verification) the email service provides, practicing good email security and privacy habits are important to ensure that no else can sign into your email account or see your email.

- **Use secure devices**
  Try not to log into your account on devices (smartphones, tablets, computers) that the perpetrator has access to or is monitoring. Depending on how the device is being monitored, the person monitoring it may know your email address and password.

- **Always log out**
  Whenever you log into your email account, whether it is on your own device or on someone else's (at the library for example), always log 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 will be helpful in case someone picks up your phone or computer or you lose it.

If you check your email on your smartphone 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. You can make sure your phone or laptop is secure and that others can't access it without your knowledge. 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 traveling 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 browser or smartphone 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. In this case, it doesn't necessarily remember the password, but your email account is "remembered" in the web browser. The next time you (or anyone else) opens 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 smartphones 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 + passwords. If you are concerned that someone else may have access to your devices, don't allow it to store your passwords. This may be convenient for some less sensitive accounts, such as your Netflix log-in, but for your email account, you want it to be secure.

- **Be cautious when giving out your email address**
  Since email addresses are what people use to contact you, you will need to give it to people. However, you may not want to give out your email address to everyone who asks, particularly to stores or set 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 smartphone service.

Some email services let you create short-term email accounts. These email addresses lasts 10 minutes to 24 hours, so it's very temporary. Generally, the way these work is the service assigns you or you create a temporary email address. 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 basically acts like 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.

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

Adapted from and in cooperation with the WESNET Safety Net Australia project at the Women's Services Network, Australia