10 EASY STEPS TO MAXIMISE PRIVACY
#KNOWTECHABUSE

Please note that the contents of this document should not be regarded as legal advice. The information covers general technology safety information and may require safety planning before making technology safety changes depending on each survivor's situation. Trust your instincts and use a safer device, one that has not been accessed by an abusive person, to contact a domestic and family violence specialist service if you have concerns for your safety. The information contained within is relevant as of February 2020.

We live in a world of constant technology use and lots of sharing. Technology has made it easier for families, friends, co-workers, and long-lost classmates to connect, and our online lives have become just as important to us as our offline ones. But what you share doesn't always stay within those circles and can be shared much more broadly than expected. Sometimes our technology gets out of our control. So what can you do? Here are some quick ways to ensure that your tech use and sharing is done a little bit more safely.

1. Log out of accounts and apps

You'd be surprised at how many people forget to log out of their accounts. They only realise they forgot when someone else posts something outrageous on their timeline or feed. Logging out of your account is even more important if you're using someone else's device or a public access computer. Uncheck the 'keep me logged in' feature and decline when the web browser prompts you to allow it to remember your password to automatically log you in next time. Failing to do this will make it easier for anyone to pick up your computer, tablet or smartphone and post away, pretending to be you.

2. Use strong passwords

Use strong passwords to prevent other people from accessing your accounts. We recommend using a different password for each account, rather than a password that someone who knows you can easily guess or a one-word password that can be easily cracked. Create a system so that you use unique passwords that only you will know, consisting of, for example, at least 10 characters and letters in both uppercase and lowercase, and in combinations of letters, numbers and symbols. You might consider using a reputable online password manager, accessible by inputting one password only, that can save and store all your important usernames and passwords as well as generate rock-solid unique passwords, if required. It may be less secure to use your browser to save your passwords. Finally, use 2-factor authentication so you are notified when someone is trying to access your account.

3. Review privacy settings on all apps and accounts

Review the privacy settings on all your online accounts, particularly your social media ones. Most sites allow users to limit what others see, whether it's status updates or profile information. Don't forget that it's not just Facebook, Instagram and Twitter that have privacy settings. Most online accounts, such as Amazon, allow you to limit who can see your profile information.

4. Minimise location sharing

Smartphones, smartwatches, and linked devices such as Bluetooth and wireless headphones can have location-sharing capabilities. You could be sharing your location without even knowing it. You can control which app has access to your location by turning off that option through your smartphone settings (most phones have location privacy options in the settings). Some social media platforms also allow you to manage your location privacy through the site's privacy settings.

5. Don't include location coordinates in your pictures

Did you know that when you post a photo taken on your smartphone or camera that you could inadvertently share your location as well? That means that the selfie you just posted and uploaded online could contain your address or exact GPS coordinates. You can turn off that 'geotagging' capability through the privacy settings on your camera app. Don't forget that even if you turned off the location option for your camera app, the photo sharing or social media app that you're using may share your location - so turn off the location option for the app as well. You can also delete the location data from photos taken with the location settings on by going to 'properties' on the digital photograph and manually deleting the information.

6. Be mindful about logging into accounts using other accounts

Connecting your Instagram to your Facebook, or other social media platforms may make it easier to update everyone following you with just one click, but that also means that a lot more people will have access to a lot more information about you. It also makes it more difficult to lock down your privacy. For example, if someone gains access to one account they may be able to access your linked accounts.

7. Be careful when using free wireless networks

Free internet is great, but you pay for it by being more vulnerable to risks. Using open wireless networks at your local coffee shop or sandwich shop can leave you susceptible to hackers accessing your private information. If you're going to check bank accounts, buy something where you have to give your credit card information, or do anything sensitive, wait until you are back on a secure network. And if your personal hotspot or wireless network at home doesn't have a password on it, it's a great idea to put a password on it now!

8. Use HTTPS everywhere

Not all websites are created equal. Some sites are more vulnerable to viruses, and when you visit them, it makes your computer or device more vulnerable. However, some sites have a secure version. You can tell by looking at the link in the URL address bar. If it starts with 'https', it's a secure page vs. 'http', which is just a normal page. The next time you're checking your bank account or buying something online, check out the address bar. Browsers often show a closed lock symbol or green colour to indicate it's a secure site. An easy way to ensure that you're using the secure page whenever you can is to download the HTTPS-everywhere browser add-in. Each time you go to a site, it will try to open the secure (https) site rather than the normal one. If the site doesn't have a secure page, it will default to the normal page.

9. Use Private Browsing, Incognito or InPrivate Browsing

You can choose to browse the internet privately in Google Chrome, Mozilla Firefox, Microsoft Edge and Safari. Basically, private browsing means that someone can't open your web browser after you've used it and go through the history to see which sites you visited. Browsing privately is safer if you're using a friend's computer or tablet or are on a public computer. Be aware that you have to close the browser to erase your history. If you leave it open, users after you can still see your browsing history.

10. Use more than one email address

Email addresses are free, so have as many as you want! You can use one specific email address with a super strong password for your banking and shopping. Use another email for all the junk mail and accounts you have to create in order to use a particular web service. You

could even consider using different email addresses for different social media accounts. Using different emails for different accounts is safer because if someone guesses one of your email and password combinations, they don't get access to all your accounts. You can even go one step further and download a service that 'masks' your account address, so that you're never using your actual email address.

Trust Your Instincts

If you are living with abuse or have separated recently, it may not be the safest option to update your passwords or take extra privacy steps. You know your situation best so *trust your instincts*. If it's going to make the abuse escalate then perhaps leave those steps for now and get some support and safety planning ideas from a domestic and family violence or sexual assault specialist service.