Bourne Secure

https://bournesecure.com

Hello to all of my fellow Dorset Humanists!

This guide follows on from the talk I gave to Dorset Humanists on 24/2/2021 and includes information which will allow you to improve your online privacy and security. Although this document mentions topics like computer viruses, hackers, scams and other risks to your digital privacy, I don't want to give the impression that the internet is such a scary place that it's something to be afraid of.

The internet is a wonderful tool, and although a breach of information confidentiality is a possibility when using computers, I hope that you will feel reassured that by using this guide, the risk to your information will be dramatically reduced, and perhaps by using this information you will feel more confident online.

All the best,
Daniel Dancey

Privacy

Who does this guide protect your information from?

Companies

This online privacy guide is intended to help you to reduce the amount of information that you allow to be collected by large companies online. It's entirely up to you to decide how much information about your digital life you are willing to share with companies. Many people are perfectly happy with all of their data being processed by these companies, and I don't think that they're wrong in this decision, just that I think it's important to think about what's right for you.

These are some of the reasons that somebody might choose to restrict the information that companies can collect on you:

- Some companies like holiday booking agencies charge customers more when the information they hold on them indicates that they might be able to afford paying more.
- Companies like to advertise to people who they think will be the most profitable customers, while avoid those customers who they perceive as not being as profitable. This has led in the past to situations like housing associations excluding minority groups from seeing adverts for the housing they provide. A person who companies have identified as having lower financial means may see more adverts for high interest rate loans.
- Somebody using a digital service provided by a company may not understand the privacy settings, and their activity or communications using that service may be visible to a wider audience than they intended for.
- There is a small chance that information held by the company will be stolen by hackers in the future. The risk of this with large organisations like banks or powerful tech companies is very low, although less well resourced businesses may be vulnerable to this.
- The information may be data mined by the company to reveal additional data points that you might not have intended for them to have access to.
- Some people feel uncomfortable with private information being collected simply because they dislike the idea of that information being accessible to someone else, even for business purposes.

Individuals

Some of these steps involve tightening the privacy settings on websites to restrict the audience with which you share your activity or communications. This does not prevent the companies hosting

these services from using that information, but it would restrict access from people online who you have not approved.

One example of someone who you might like to keep this information from could be a prospective employer who you don't want to discriminate against you based on personal information you've put online.

There are also some people online who attempt to profit from misleading other people into downloading a virus or by stealing financial information. One way that they might do this is by sending a message which purports to be from a bank or other trusted organisation, but is actually a forgery intended to trick the recipient into handing over login information or sending money. While this may sound scary, it's actually quite easy to spot and these interactions are completely harmless when you know how to avoid them, as described in the "avoiding common scams" section later in this document.

I do not believe or intend that the information contained within this guide would protect your information from nation state backed entities, as such a guide would likely be much longer than 6 pages. Unless your name is Edward Snowden or you are living in a repressive regime, this probably won't be of any practical concern to you, though.

Step 1: Assess what information you have already put online. Many companies have automated systems for giving you access to all the information they hold on you, although the meaning or importance of some data may be unclear outside of the context of the database it's stored in. If a company does not have an automated tool, you have a right to make a Subject Access Request to ask for access to the data they hold on you. https://www.which.co.uk/consumer-rights/advice/how-do-i-make-a-subject-access-request

Consider how someone like the curious prospective employer mentioned earlier would find information about you and go through those steps yourself to see what might be publicly available.

Search for your name on all of the major search engines and social media sites, and make sure to look beyond the first page. If you are finding too many options of people with the same name as you, try including your town in the search terms to narrow the results to your own records. Including snippets of information like the postcode may show you areas where your address has been listed online. Searching for your email address or previously used usernames may also reveal interesting information.

haveibeenpwned.com will tell you if any of your existing accounts have been involved in a data breach, so you can change the passwords for those accounts.

Step 2: Decide how much information you are comfortable with sharing, and with who. Consider that information you have shared with companies or within private online spaces may inadvertently or maliciously one day be shared with a wider audience than you intended.

Step 3: Delete information that you have previously posted online that you are no longer comfortable with being publicly available. If you are unable to remove any information, you may consider using the "right to be forgotten" if it applies to your situation. https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/

Step 4: Restrict your privacy settings with apps and services to better reflect the audience that you are comfortable sharing with. This means going into the user preferences menus on each of these services and looking at the privacy section to see which choices you are able to make about their

use of your data. Social media sites make this relatively easy to do, and often have a setting to retroactively apply the changes to previous posts you've made on their services.

Enable "Do Not Track" in your web browser privacy settings and enable Tracking Protection in your browser if it's available.

Step 5: Switch to using services which respect your privacy and who provide tools to protect your information. End to end (sometimes called point to point) encryption is the best kind, as it prevents the companies involved in transporting your data from being able to access it. The easiest changes to make in this list have been highlighted below using italics, with the remaining three options involving a degree of inconvenience.

- *Use Firefox instead of Chrome or Edge.*
- *Use DuckDuckGo, Qwant and Startpage.com instead of Google search.*
- *Use Signal for instant messaging instead of Facebook Messenger, Skype or similar.*
- Consider deleting your profiles on websites that do not respect your privacy, such as Facebook.
- Use ProtonMail for email instead of Gmail.
- Consider using free and open source software like LibreOffice instead of Microsoft Office. Part of this choice is a financial one, it doesn't cost any money to use LibreOffice whereas Microsoft charges a fee for their products. If you haven't yet purchased Microsoft Office or if you're making ongoing payments towards their subscription service version of it then you will likely benefit the most by choosing LibreOffice instead.

Step 6: Change your online behaviour so that in future you only share the information online that you've decided you're comfortable with, continuing to use the more privacy respecting solutions you chose in Step 5 and avoiding services like Facebook that don't respect your privacy.

Periodically assess the success of your strategy by looking yourself up online like you did in Step 1 and make changes to your information sharing policies if you find that your information is still more widely available than you are comfortable.

Other notes:
Cookies - Set your Firefox browser to reject third party cookies and learn to reject advertising cookies when you access websites. Some websites are incorrectly configured and ignore your request not to set advertising cookies, so periodically clear your browser cookies. Keep in mind that this will log you out of websites, so be prepared to log back into some sites afterwards.

Plugins - Installing the "uBlock Origin" and "HTTPS Everywhere" browser plugins will improve your privacy and security.

VPNs – VPNs can be useful tools, although it's possible that free VPNs might themselves steal and sell your data. NordVPN seems like a fairly trustworthy service. The main advantage of a VPN is being able to access region locked content like American Netflix, and the privacy advantages only really apply for accessing websites that don't support HTTPS.

Private Browsing mode is worth using and understanding. When you access a website using private browsing, it usually doesn't know who you are until you log in and no information is saved after you close the browsing window.

WhatsApp has been in the news recently because they have started giving information about who you're talking with to Facebook. Switching to Signal is probably a good idea.

Email accounts – Using a different email account to sign up to different categories of online services is sensible. You could use one email account for business, one for online shopping, and one for social media sites.

Security

Related to the subject of digital privacy is computer security. Having your information extracted from your computer or damaged via malware could undo all of the good work you've done in the previous steps.

Keep in mind that these steps will improve your security, but will not make you completely invulnerable to a breach in security. Try to consider the risk of any action as being the level of damage that a breach would cause multiplied by the likelihood of that breach actually occurring. If you follow these security steps then the likelihood of a breach will be somewhat lower, perhaps beyond the abilities of a low resourced attacker, but still far from impossible.

Avoiding common scams

HMRC or Microsoft will never phone you to ask you to log into your online banking. Sometimes these scammers ask you to download some software and say that they will be paying you a refund via your bank, which ends with them pretending to have given you too much money and demanding that you give it back via gift cards. Just hang up on these scammers.

Other scams include attempts at blackmail where an attacker contacts you pretending to have already hacked you and stolen data, demanding payment to avoid them publishing it online. There is no benefit in paying these scammers, don't even reply to their emails. If they show you previously used passwords, they likely got them from a data breach on a website you've used in the past, and you are still safe if your other websites use different passwords.

An attacker might send an email claiming to be from your bank or a large company like Amazon, trying to trick you into downloading a malicious file or clicking on a link to a fake version of that website, for the purpose of stealing your password for that website. There are several steps you can take to protect yourself from this.

- Don't click on links in emails. If for example Amazon emails you saying that you have to take an urgent action on your account, go to Amazon directly in a new tab and see if Amazon has contacted you there about it. If you're unsure, contact the company directly.
- Be suspicious of urgency. Many scammers will tell you that you have to complete an action immediately, referencing their email "FINAL WARNING – TAKE ACTION TO AVOID ACCOUNT CLOSURE". This kind of wording makes people afraid to lose their account, and people act more impulsively and less rationally when they are afraid. Real companies will never demand that you do anything immediately. Again, if you're unsure, contact the company directly.
- Does the email look professionally written? A real company is unlikely to send an email filled with spelling mistakes and will likely address you by name. Scammers often put deliberate spelling mistakes in their emails because they send out millions of them, and putting in spelling mistakes filters out some of the people who reply to the email who might otherwise be too intelligent to fall for the later stage of the scam and who might waste their time.
- Don't download attachments from emails or messages you weren't expecting to receive. There have been a lot of viruses that send messages to every contact on a persons email or facebook account with what looks like a video, but that is actually the virus spreading itself when the target clicks on what they think is a message from their friend. A recent example contained what looked like a blurred explicit video with the text "is this you?", which

tricked a lot of people. A good response to this would be to contact the person who seems to have sent you the message to ask if they actually sent it themselves, and let them know that their account has been compromised in some way. Malware is often sent with a filename that ends with .exe, but it's possible to disguise malware in almost any kind of file.

Computer repair
If you need maintenance performed on your computer, consider that your local computer repair shop might not be a trustworthy source of help. There may be nothing stopping them from looking through or even copying your data. Some steps to mitigate this would be picking a computer expert you know you can trust, asking to watch them perform the maintenance and removing the storage drive or using full disk encryption before giving it to them if the work is purely hardware based.

Avoiding phishing websites
Check the URL at the top of your web browser to make sure that you're accessing the real version of websites. Scammers may carefully craft an email to make it look like it's coming from a legitimate website, but the web address linked in the email will be something like: "https://amazon.com-login.secureaccounts.com/login". In this example, the real website is "secureaccounts.com" owned by the scammer, and the part of the URL that looks like it comes from Amazon is actually just a subdomain owned by the attacker as part of the scam. It's easy for the scammer to make the website look exactly the same as the real version of the site.

An easy way to detect this is to understand how Firefox highlights the domain name (the part of the URL that says who owns the website) in the URL bar. In the example below, Firefox prints the "natwest.com" part of the url in a darker black than the rest, letting me know that I am on the real Natwest website.

Passwords and 2 Factor Authentication
Use a different password for every account you own, making sure that each of those passwords are of a high quality. Most passwords that you come up with yourself like Happydog123 are actually extremely insecure and can be broken by brute force relatively quickly, so the best strategy is to use a password manager (KeePass, LessPass and LastPass are all good options) and let it automatically generate different, randomised passwords for each site for you.

Of course you still need to create a high quality password that you can remember to log into your password manager. An example of a high quality memorable password would be "flight.emotional.receipt.storage.paperback". This kind of password would take an attacker an impossible length of time to crack and can easily be memorised and typed in quickly.

A tip to memorise this kind of password quickly if you're struggling is to create a scene or story using the words. If I wanted to memorise the password "flight.emotional.receipt.storage.paperback", I might imagine a scene where I'm in the cargo bay of an aircraft, angrily asking for my money back (using the receipt) for a storage container full of paperback books. It's a silly story, but that actually makes it a bit easier to remember.

Remember that the answers to your recovery questions on websites can be used to gain access to your accounts, and use strong passwords as the answers to those questions instead off the real answers. Your mothers maiden name is not a secure method of verification, as it's not a secret. An attacker can simply check out the last name of your uncle on Facebook to discover it.

People are often encouraged to change their passwords regularly. This is to lock out attackers who have gained access to your account to limit the time window in which they can perform harm. If you are using strong, different passwords for every site then you're less likely to have your password for any one site stolen, but it's still sensible to change them every once in a while, perhaps once a year in case you end up being a victim of phishing or somebody simply watching you over your shoulder as you enter a password.

If an online service has 2 Factor Authentication available, you should use it. This involves the company sending you a text every time somebody tries to log into your account, and that text includes a unique code that you enter into the site to prove that you still own your phone. Make sure that your phone is locked with a pin (not 1234) and doesn't display the content of text messages on the lockscreen.

SIM Jacking
Contact the company that provides your phone service and have a conversation with them about security, making sure that they have a policy of asking you for your password every time you contact them. Celebrities have had their data stolen in the past by hackers calling up phone companies, impersonating the celebrity using publicly available information and requesting a new SIM card, which they then use to recover accounts and steal information.

Recovery
A big part of your information assurance plan is the ability to recover from a breach, as even the most secure computer system could still be damaged by flooding or fire in the real world. Back up your data, and consider using offsite backups to protect your data in the event of a house fire. You should be confident that if your hard drive suddenly broke or ransomware encrypted all of your data, you won't have lost the only copy of your most valuable information.

Encryption
Considering the possibility that you will leave a hard drive or laptop behind on a bus, or that they will be stolen from your house or bag, you should learn to encrypt your data and operating system. Veracrypt is a good option for Full Disk Encryption as well as for creating encrypted volumes. Here's a video on how to use Veracrypt: https://www.youtube.com/watch?v=R-BLZ38d_-A

Warning: Veracrypt is a powerful tool, and setting up full disk encryption has the possibility of making your data permanently inaccessible if you forget the passphrase or make a mistake during setup. A common problem when entering the passphrase on boot is that the keyboard is read in US mode at that stage, so it may expect special characters to be in different places. If you are unsure, this is a step that you might consider hiring an expert to help you with.

Ask for help
If you are a computer novice, you are more likely to be tricked into downloading a virus or being a victim of phishing. There are lots of classes available where you can improve your computer proficiency, and it's likely that your bank will offer a free one-on-one service where they'll teach you to use online banking safely as well as general computing skills.

I do offer assistance with all of the subjects mentioned in guide, so if you would prefer to contact me for help, a link to my website is at the top of this website, or you can contact me through Dorset Humanists. I would like to note that this guide is not all encompassing, but following these security tips should give most people a good level of security.