BeTECHSavvy
Securing Your Digital World

NATIONAL TRADING STANDARDS
Scams Team

How to keep your digital self & data secure in a connected world

20 steps to take NOW

Incorporating Umbrella Consulting

Introduction

This checklist highlights 20 steps you can take now to keep your digital-self secure; your digital identity, privacy and data are more at risk every day.

Learn to take control of your digital self, in the same way that you would take control over your personal health, or your savings, or your right to vote.

Hi... My name is Ben Hill and I am the founder of BeTechSavvy. I have always had a keen interest in computers and have over 20 years of experience in IT, on numerous different Operating Systems, operating in various environments.

Having a productive and safe online digital life is important for you and your family to get the most from online experiences. With the amount of information that we share online, it is important that we retain the ability to define the boundaries of our digital lives. While many people already have their own go-to tips and tricks, for others, identifying a pragmatic approach to digital privacy and security might seem overwhelming.

I will give honest free advice on a range of problems that people experience with physical device security, Wi-Fi connectivity /security, data handling and security.

I am also able to provide practical support and training to customers... so feel free to speak to me!

Benjamin Hill

CEO & Founder

Online identity theft & cybercrime is on the increase, how do I keep myself safe when accessing sites on the internet?

1. Browse the internet securely

Make sure HTTPS is enabled by looking for the green lock in your URL bar when browsing the web. HTTPS encrypts your data as it travels to and from the website, you're visiting to ensure it remains private. You can consider installing a HTTPS extension for your web browser to enforce this wherever possible.

If your antivirus does not protect your online identity (most paid versions offer this), then consider using a separate secure browsing/sandbox service; keeping criminals away from the browser and prevent the theft of any personally identifiable information.

Avoid clicking on links or attachments: Cybercriminals do a good job of tricking people into clicking on links supposedly from their bank, telecom operator, electric or gas company, tax service and other legitimate organisations. Think before you click – spelling errors, email addresses that do not seem right, and out-of-the blue or unusual communications from friends should be treated with utmost caution. In doubt, call the organization or your friend to verify before clicking.

2. Use unique passwords for every login

Passwords are the keys to your digital kingdom: Use unique, complex passwords with a combination of lower and upper-case letters, numbers and symbols and do not use the same password across your accounts.

3. Use a password manager

Instead of trying to remember various passwords, or where you wrote them down, use a password manager to do this for you. A password manager is a piece of software that uses **one** *tough-to-memorise (but tough-to-crack)* password to store all your other passwords. As you navigate the web, you only have to memorise one password and your password manager will do the rest.

Most password managers allow you to create a unique and strong password for every account that will pass the security requirements for a site. There are several particularly good free password managers. Paid password managers generally offer more features, however.

4. Parental control IS important

With children accessing more and more content online, they become more susceptible to targeting of people who want to use their identity and data for nefarious reasons. Sometimes we let our kids **use** devices because we're looking for a few minutes to get something finished. Setting time limits and doing spot checks (verbally or with digital parental control is important). Most Operating systems have parental control options built-in. Use them if you have children!

How do I keep my data secure whilst accessing the internet?

5. Install an antivirus and keep it updated

We call this type of software antivirus, but it protects against all kinds of malicious software. Ransomware encrypts your files and demands payment to restore them. Trojan horse programs seem like valid programs, but behind the scenes they steal your private information. An effective antivirus protects against these and many other kinds of malware.

There are numerous Antivirus companies out there, that offer limited free of paid, fully functioning protection. It is down to personal preference as to whether you pay for full protection or use the basic/free versions instead. One more thing. If your antivirus or security suite does not have ransomware protection, consider adding a separate layer of protection. Many ransomware-specific utilities are entirely free, so there's no reason not to try a few of them and select the one that suits you best.

6. Get a VPN and use it

Use a VPN, Tor, or similar tools to help protect your online activity. These tools serve as protective layers by routing your traffic through multiple computers, making it difficult to trace your digital footprint and enhancing your safety online.

A VPN encrypts your internet traffic, routing it though a server owned by the VPN company. That means nobody, not even the owner of the free Wi-Fi network, can snoop on your data.

Using a VPN also hides your IP address. Advertisers and trackers looking to identify or geolocate you via that IP address will instead see the VPN company's address. Spoofing your location using a VPN server in another country can also serve to unlock content that's not available in your own region, i.e. Netflix, BBC iPlayer etc.

Be cautious while on public Wi-Fi by disabling sharing, using a VPN (Virtual Private Network), and enabling a firewall.

7. Use Two-Factor Authentication where it is offered

Use two-step login, especially for important personal accounts, such as email and online banking. Two-step login is when you configure your account to enter a one-time code in addition to your password. This code can be retrieved via text message, standalone token, or an app on your phone. Enabling two-factor authentication for your password manager is a must.

What other precautions should I take to protect my data?

8. Use Passcodes Even When They Are Optional, Especially On Mobile Devices

Password-protect and/or encrypt your devices, assuring that even if your device is lost (or worse yet, stolen), your information is secure.

Many smartphones offer a four-digit PIN by default. Don't settle for that. Use biometric authentication when available, and set a strong passcode, not a stupid four-digit PIN. Remember, even when you use Touch ID or equivalent, you can still authenticate with the passcode, so it needs to be strong.

9. Data encryption

Just as important as it is to back up data, it is important to protect the privacy of your stored data. Whether you send data over any network or look at it on your device at home, data encryption ensures that your files stay safe and locked. Most Operating systems allow versions to encrypt data on the device. Android and iOS for example, automatically encrypts a device and the data in. Mac OS has a built-in volume encryption technology called FileVault. Window uses Bitlocker (but not in their 'Home' version). These should be enabled immediately, if not turned on!

There are various free software offerings available to encrypt files and/or folders, whether they are stored on your device or in cloud storage. I would recommend encrypting important data in the cloud, in the same way that you would protect data on your physical device.

10. Back-up your data

If your computer is infected by ransomware, malware or it crashes, the only way to ensure that you will be able to retrieve your lost data is by backing it up and doing so on a regular basis. This also means that if you mislay data or accidentally delete something, it can always be recovered.

Back up your data on external devices or a cloud platform. A cyber attacker could compromise your computer's operating system, or your data may be wiped out by a hardware failure, corrupting your personal information.

11. Pay with your smartphone

The system of credit card use is outdated and not very secure at all. That's not your fault, but there is something you can do about it. Instead of whipping out the old credit card, use Apple Pay or an Android equivalent everywhere you can.

General housekeeping tips to protect your data

12. Update your software frequently

Keep all software on your PC up-to-date with the latest updates and patches. Not only do updates provide newer functionality, but a software provider will usually identify and fix bugs or exploits and will provide a patch or update to mitigate these exploits. By keeping your software up-to-date, potential vulnerabilities (including zero-days) can be patched and help keep cybercriminals and hackers at bay.

13. Risk awareness

Avoid using publicly-available USB ports and plug in your own charger. Our devices are configured to transfer/sync data when directly connected to USB ports, making them more susceptible to data theft.

Securing your smart home and Internet of Things devices

14. Give your router a name

Don't stick with the name the manufacturer gave it — it might identify the make or model. Give it an unusual name not associated with you or your street address. You don't want your router name to give away any personal identifiers.

15. Use a strong encryption method for Wi-Fi

In your router settings, it's a good idea to use a strong encryption method, like WPA2, when you set up Wi-Fi network access. This will help keep your network and communications secure.

16. Set up a guest network

Keep your Wi-Fi account private. Visitors, friends and relatives can log into a separate network that doesn't tie into your IoT devices.

17. Change default usernames and passwords

Cybercriminals probably already know the default passwords that come with many IoT products. That makes it easy for them to access your IoT devices and, potentially, the information on them. Are you considering a device that doesn't allow you to change the default password? Then consider a different one. Always use strong, unique passwords for Wi-Fi networks and device accounts.

18. Check the setting for your devices

Your IoT devices might come with default privacy and security settings. You might want to consider changing them, as some default settings could benefit the manufacturer more than they benefit you.

19. Disable features you may not need

IoT devices come with a variety of services such as remote access, often enabled by default. If you do not need a feature or function, be sure to disable it.

20. Audit the IoT devices already on your home network

It could be time to upgrade that old security camera. Take time to check if newer models might offer stronger security.

---- Remember ----

“Technology trust is a good thing, but control is a better one.”

Stephane Nappo