

# CYBER SECURITY



**Before commencing this article published by Norton Security we point readers towards the UK's National Cyber Security Centre ([www.ncsc.gov.uk](http://www.ncsc.gov.uk)); in particular, the section that deals with Individuals and Families. That section explains what cyber security is, provides cyber aware top tips, deals with common cyber problems, advises how to protect data and devices, and how to report cybercrime.**

*"You might think that the only form of cybercrime you have to worry about is hackers stealing your financial information. But it may not be so simple. There are far more concerns than just basic financial ones. Cybercrime continues to evolve, with new threats surfacing every year.*

*When you hear and read about the range of cybercrimes out there, you might be tempted to stop using the internet entirely. That's probably too drastic. Instead, it's a good idea to know how to recognize cybercrime, which can be the first step to helping protect yourself and your data. Taking some basic precautions and knowing who to contact when you see others engaged in criminal activities online are also important steps. Furthermore, you might want to learn how to prevent cybercrime, but here's the thing: You can't. You can, however, take precautions to help protect against it.*

## ***What is cybercrime?***

*Cybercrime is any crime that takes place online or primarily online. Cybercriminals often commit crimes by targeting computer networks or devices. Cybercrime can range from security breaches to identity theft. Other cybercrimes include things like "revenge porn," cyber-stalking, harassment, bullying, and child sexual exploitation. Terrorists collaborate on the internet, moving terrorist activities and crimes into cyberspace.*

## ***How to protect yourself against cybercrime***

*Anyone using the internet should exercise some basic precautions. Here are 10 tips you can use to help protect yourself against the range of cybercrimes out there:*

### ***1. Use a full-service internet security suite***

*One that provides real-time protection against existing and emerging malware, including ransomware and viruses, and helps protect your private and financial information when you go online.*

### ***2. Use strong passwords***

*Don't repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.*

### ***3. Keep your software updated***

*This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.*

### ***4. Manage your social media settings***

*Keep your personal and private information locked down. Cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.*

### ***5. Strengthen your home network***

*It's a good idea to start with a strong encryption password as well as a virtual private network. A VPN will encrypt all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data. It's a good idea to use a VPN whenever you use a public Wi-Fi network, whether it's in a library, café, hotel, or airport.*

### ***6. Talk to your children about the internet***

*You can teach your kids about acceptable use of the internet without shutting down communication channels. Make sure they know that they can come to you if they're experiencing any kind of online harassment, stalking, or bullying.*

### ***7. Keep up to date on major security breaches***

*If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.*

### ***8. Take measures to help protect yourself against identity theft***

*Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. How? You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That's why it's important to guard your personal data. A VPN — short for virtual private network — can also*

help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

**9. Know that identity theft can happen anywhere**

*It's smart to know how to protect your identity even when traveling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and using a VPN when accessing the internet over your hotel's Wi-Fi network.*

**10. Know what to do if you become a victim**

*If you believe that you've become a victim of a cybercrime", see: [How to report cybercrime in the UK | CSO Online](#)*



See also: [How to protect yourself against scams, from phishing to romance fraud \(telegraph.co.uk\)](#)

[www.aerospacecareersprogramme.co.uk](http://www.aerospacecareersprogramme.co.uk)

