

THE LITTLE LEAFLET OF

# CYBER MISTAKES



**METROPOLITAN  
POLICE**


NEW  
SCOTLAND  
YARD

## MISTAKE 1: HAVING A WEAK PASSWORD

**Your password is the lock on your door. Make sure it's strong.**

! Simple passwords can easily be guessed by criminals. Don't use words personal to you (sports teams, pets, family etc.), never share it with anyone and use a separate password for your email.

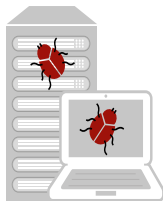
sam~~x~~dog    englan~~x~~1966    passw~~x~~d123    qw~~x~~ty

fishboattulip 

**To create a stronger password, join three random words together. Then add numbers, symbols and uppercase letters. For example: 19fisHboaTtuliP95!!**

## MISTAKE 2: NOT HAVING ANTIVIRUS

**Antivirus is your security guard. Make sure you have some, and that it's up to date.**



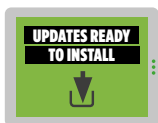
! Viruses and malicious software (malware) can infect any device (computers, phones, etc.). Once it's there, it can lock you out, steal your information or even watch you in your home!

**Most systems have anti-malware already built in. Make sure you're using it. Also consider installing extra antivirus on all your devices (which can be free). Both of these act as a security guard, checking everything that tries to come in. They will alert you if anything tries to infect your system.**



## **MISTAKE 3:** **NOT UPDATING SOFTWARE**

**Vulnerabilities are holes in your walls. Updates and patches fill the holes in.**



Software is never perfect. Often it has vulnerabilities or holes that criminals can use to get inside. When one is found, the software is updated or patched to remove the problem.

**Always update or patch your software as soon as you're prompted to ensure that it remains safe and secure.**

## **MISTAKE 4:** **NOT BACKING UP DATA**

**Make copies of things that are important to you. Keep them safe.**

Your files, contacts and memories are some of the most important things on your computer. If your computer were to break, or become infected, having a safe backup means you don't lose them.

**Regularly copy your important information to multiple external locations (hard drives, thumb drives, cloud etc.).**



## **MISTAKE 5:** **CLICKING ON LINKS AND ATTACHMENTS**

**You wouldn't let a stranger into your home. Why let them onto your computer?**

Emails you receive may contain attachments or links you are asked to click on. Doing so could allow criminals to install malware, giving them complete control of your device.

**Don't click on links unless you can verify where they came from. If in doubt, call the sender to check it's genuine.**



## **MISTAKE 6:** **SHARING EVERYTHING ON SOCIAL MEDIA**

**You wouldn't take an advert out to say you're going on holiday and your house is empty. Why tell the world via social media?**

⚠ Social media is great to keep in touch with friends and family, but unless you've checked your privacy settings, you might be telling more people about your life than you intend.



**Be careful who can see what you share online. Ensure your privacy settings on social media are set to a high level.**

## **MISTAKE 7:** **TRANSFERRING MONEY WITHOUT CHECKING FIRST**

**You wouldn't hand out cash to people on the street without checking who they are. Why do so online?**

⚠ Criminals can easily pretend to be anyone online. They can mimic emails, websites and phone numbers of your friends, colleagues, customers or banks. They'll try and trick you into transferring money into their bank account.



**Always verify requests for payment, or alteration of bank details directly. Find contact details from another source, and don't transfer until you can confirm who you're sending it to.**

---

Always report fraud and cybercrime to Action Fraud, either online at **[www.actionfraud.police.uk](http://www.actionfraud.police.uk)** or by telephone on **0300 123 2040**.

For practical advice on how to protect yourself and your business online visit **[www.getsafeonline.org](http://www.getsafeonline.org)**

To contact the Metropolitan Police cybercrime prevention team email **[cyberprotect@met.police.uk](mailto:cyberprotect@met.police.uk)**