Fidelity
INTERNATIONAL

Cybersecurity for less confident computer users

Help and advice for staying safe
online at home and on the move

What is cybersecurity?

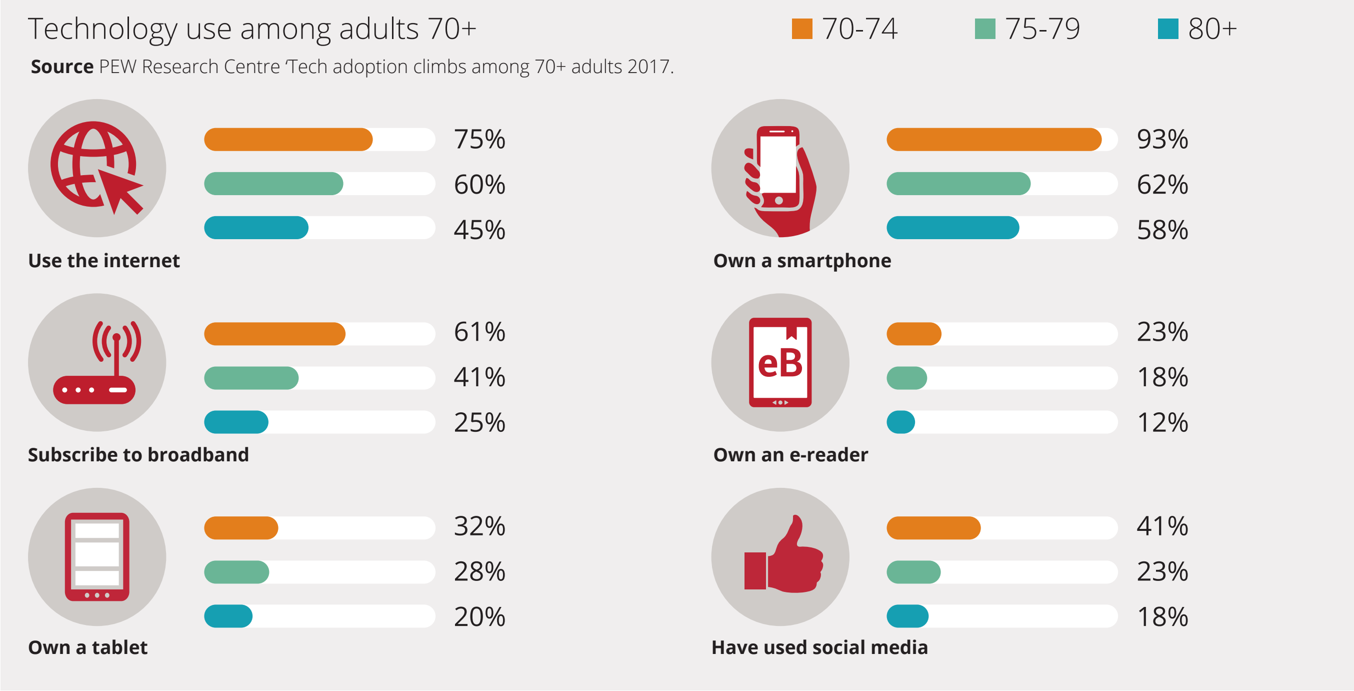
Cybersecurity is the name given to the approaches and methods that anyone can use to protect themselves from fraud, identity theft and any other form of online or electronic crime.

It could just as easily be called *General Internet Safety* or *Good Computer Hygiene* too, as it's the way we protect, not just ourselves, but anything that's connected to, or accessed by, the Internet. From the data stored on your own computer, phone or tablet to the details you type into the websites you visit, your shopping history and the news and information you share with friends and family online.

You don't have to be an expert to recognise the ways in which the internet has changed the world over the past 25 years.

A virtual world snapshot

If you look at the statistics of internet users, worldwide you'll see that the 18-34 age group makes up the largets group, no surprise there perhaps, but the *fastest growing* demographic? Those aged 65 and up...



Technology use among adults 70+

Source PEW Research Centre 'Tech adoption climbs among 70+ adults 2017.

Computers have brought us all so many benefits; from email, instant-messaging and online shopping, travel-planning, banking and 'virtual' meetings to the now ubiquitous 'social media' websites, which allow us to stay connected, informed, and involved with family and friends; wherever they, or we, are in the world. The rate of change only continues to speed up.

Which is why cybersecurity is so important because, while the Internet brings us many conveniences, it also comes with risks. The new, 21st century technologies and resources have bred a new species of crime; cybercrime.

Online criminals can appear as friends or family members, banks, mortgage vendors, charities, and even healthcare

When banking and shopping online
Make sure the website address you've banking or shopping with starts with "https," (the 's' stands for secure) and check for a padlock icon, either at the bottom of your browser or in the address bar, like the one shown to the left here.

and low-cost prescription providers, all in order to steal your information and identity, commit credit-card fraud and simply conduct some old-fashioned theft from your bank account.

If you are a user of modern technology it's not just in your interest to learn about cybercrime, it's your responsibility. It's every bit as important as understanding how to use the latest smart phone or post on Facebook because, sadly, it's a fact that less confident computer users are a distinct target-group for cybercriminals.

It's important to think seriously about cybersecurity and get in the habit of staying aware to the risks inherent in taking part in the online environment. In just the same way that, for instance, you would never leave your home with the door unlocked or the keys left in the lock you also need safeguards to secure your computer and the data you share online. The good news is that *anyone* can minimise those dangers by making a few small changes in their behaviour, leading to smarter, safer, online decisions and a stronger, safer internet experience.

So what should you be on the look out for, and how, exactly, do criminals try to get hold of your identity and cash? Let's take a look.

What is phishing and how can we spot it?

Phishing is an attempt, usually through email, to gather personal information or to compromise technology for the purpose of financial gain or malicious activities. Phishing emails typically include a link to a fraudulent site or an attachment containing malware. Every day millions of phishing emails are sent out to unsuspecting victims all over the world.

01 **Suspicious/mismatched URL:** hover your mouse over the links in an email and you can reveal the real destination address, check the details carefully as some addresses can seem to be genuine but have subtle differences (like www.amazon.com v's www.amazon.org).

02 **Poor spelling or grammar:** When a major organization sends out a message it's usually checked for spelling, grammar, and legality, if a message is filled with spelling mistakes it probably didn't come from a reliable corporation.

03 **Asking for personal information:** like passwords: No reputable company will ever ask you to send or confirm passwords or log-on details via email, or get you to click on a link that takes you to a website where you can log-in. If you're in doubt contact them yourself to check.

04 **You're not expecting anything:** You won a big prize or competition! But did you, in fact, enter one? A financial company is 'replying' with the spreadsheet you requested, but did you ask them for anything in the first place. Chances are excellent this is a phishing email.

05 **You must act now!** Messages that say you must 'Reply Now' to avoid losing money, or having your account access cut-off, or account deleted, are usually trying to get you to act without thinking. Take your time and investigate. Don't feel rushed into doing something you shouldn't.

06 **Something just seems wrong:** It would be great if we could cover every way a phishing attack could happen here but the truth is the best defence you have against fraud is our common sense. Sometimes things just don't quite seem right, learn to trust that feeling.

If you think you've spotted a phishing email, don't just ignore it... take action. **Delete it!**

Hooked by a phish.

Phishing is probably the most common way a criminal will try to take advantage of you. 'Phishing' is the name given to an email that pretends to come from a regular, trusted sender. It may be purporting to be from your bank or lawyer, a family member or friend or someone you've never heard of, telling you that you have, for instance, won a big prize or are due a tax rebate.

The permutations are endless, the one common factor that all phishing emails have in common is this; they're a fraud.

Cybercriminals are able to copy your contacts' email addresses and send you a message that looks as if it came from them. Typically they will use a faked email communication to ask you to click on a link taking you

to a website which may look genuine but is, in fact, a clever copy, created by the criminals. Any details; like passwords or credit-card and bank-account numbers, you input into this fake website will go straight to the thieves.

Clicking on links in emails is one of the top methods criminals use to get access to your personal information, but 'fake' phishing emails could also contain viruses (called 'malware'), that could infect your computer or device, activated by something as simple as clicking on the file *attached* to an email.

When to be wary.

Emails (and any other kind of communication like phone calls and text messages) that create a sense of urgency, like a supposed issue with your bank account, pension or taxes is likely a scam. Creating a sense of panic is a good way for hackers to try to circumvent your natural sense of caution.

If you get a message of any kind that you feel is trying to rush you into something, contact the person or company by phone, on a known number - not on the number you may have been given in the suspect communication - to determine if the problem is legitimate or not. Similarly, don't open attachments, click links, or respond to any email messages that asks for your log-on (i.e. user-name and password) information or account details. No reputable bank, hospital, shop or company of any kind will ever ask you to send or input that via an email.

To be extra safe, don't join a club, enter a contest or share your personal information for any reason unless you know you are on a reputable, well-known website. And be wary of

any requests to contact any site or organisation you haven't heard of, especially if they're asking you to update or confirm personal details.

Always be particularly on your guard when receiving or replying to emails from financial institutions, internet service providers and other organizations that hold your personal or financial information. These are almost always the top choice of communiqué for a criminal to emulate.

The "free" gift, or unexpected prize or holiday is another red flag. It would be great if we lived in a world where companies were handing out free holidays all the time, but these are cheap tricks designed to get you to give up personal information. Delete them immediately, no matter how tempting the offer or how big the prize might be!

None of this means you can't go ahead an exchange emails with friends family and services, it just takes a bit of extra awareness to stay safe; If an email looks unusual in any way, even if you know the person who sent it, it's definitely best to delete it. Take a look at the '**Spotting a Phishing Email**' above for our 6 top-tips on identifying suspect messages. And remember: If in doubt, throw it out.

Weak passwords.

Passwords are difficult things, they can't be so elaborate that they're impossible to remember, but they need to be complex enough to avoid easy-guessing or hacking. Because selecting a weak password, or using the same password across multiple accounts, could leave you vulnerable your password handling need some thought...

Fidelity
INTERNATIONAL

For good security, passwords should be as long as you can realistically make them (at least twelve characters). A good idea may be to use a pass 'phrase' rather than just one word. Perhaps a line from a song or poem, or an obscure slogan or snatch of movie dialogue, whatever you choose, the longer the better. The more unusual it is, the stronger it is (and, often, the more memorable it is too!).

It should have a sprinkling of capital letters, numbers and symbols; try substituting '@' for 'a' or '$' for 's' for instance. If you can mix-in some elements from a foreign language, or even a made-up word, all the better.

However you decide on the makeup of your long, strong password one piece of advice always stands: don't include personal information, it's just not secure enough. Michael Kaiser, executive director of the *National Cyber Security Alliance*. says: "If your password is something simple to remember because it uses your child's name or birth-date, or your anniversary date, you need to create a better password."

But it's not just internet sites you should password-protect. Lock <u>all</u> your devices, including tablets and smart phones, with secure passwords or codes. It's the first and best line of defence in case you lose a device or have it stolen.

Securing access to your accounts.

If your password *is* unfortuntely guessed, hacked or otherwise stolen, then you may want to consider adding another layer of protection to your online accounts by activating what's called *two-step authentication* (also called *two-step verification*) - a process that involves two authentication methods, performed one after the other.

An increasing number of online services, apps and sites now offer this free options which helps prove that it's really you, not just someone with your password, trying to access your account. It works by including a secondary step to the log-in process, like entering a code which is automatically sent via text SMS to your smart phone, and it can significantly increase security.

Oversharing on Social Media.

Be cautious of what you share on social-media sites like Facebook, Twitter and Instagram. What you say and what you do online is visible to others, and it's permanent.

Cybercriminals use the anonymity of the Internet like a mask and are known to create fake social media profiles, which they then use to contact unsuspecting users. So don't reveal any personal information to strangers online.

Your personal information includes your name, address, age, telephone number, social-security number, doctors name, birthday or even your location, anything which could be pieced-together and used to steal your identity, take control of your accounts or find you in the real world.

Be wary of Wi-Fi

If you connect to the internet at home the chances are you're doing it through a Wi-Fi system, and that your Wi-Fi has password protection, whether you yourself entered that into your device or not. If that's the case your connection is no doubt safeguarded, but the same can't be said when you're out and about.

Be especially careful if you're accessing public Wi-Fi - at a library, cafe, hospital or similar location - it's often not secure. Don't use it for any sensitive purposes, like banking or accessing any of your online accounts. It's possible hackers have set up a system to 'capture' your details as they move across an unsecured network. Instead, if you're on the go and want to access confidential sites and enter personal information, bypass the public Wi-Fi and just use your phone's data allowance.

Always keep your devices' OS updated to the latest version
Software updates are very important because they can include 'fixes' (also called 'patches') which can solve existing security issues existing in operating systems, apps and browsers.

Update to stay safe.

You can add security to your devices by making sure that whenever you get an 'update notification' - for your smart phones operating system (OS) for instance - you install it at the earliest opportunity. Cyber criminals are constantly attempting to exploit new areas of digital technology and software developers are in a race to keep one step ahead.

Updating your OS, whether on a laptop, desktop, smart phone or tablet, will keep your device's security current.

Log out when you're done.

Remember to log out of apps and websites when you're finished using them. Leaving them open on your computer screen could make you vulnerable to security and privacy risks.

Keep learning!

Remember, the best form of protection is education; try to read-up on cybersecurity from time-to-time. Don't let yourself feel panicked by the latest cyber-threat to hit the news, be informed! You don't have to be a passive, potential victim of online crime, be proactive and stay on top of the latest scams. That way you'll be a much, much harder target and have a much, much safer online life. Thanks for reading.

Cybersecurity, a glossary of terms

Here are a few common terms and phrases you may see during your further reading and research into the subject of cybersecurity.

Source
cybintsolutions.com
16 cyber security terms that you should know.

The Cloud
'The Cloud' is the term given to the group of computers (or 'servers') with huge storage capacity that holds much of the world's data. It allows access to your files and services, through the internet, anywhere in the world.

Apps
Packages of computer software that you can install and use, most commonly a small, self contained, specific ones used for mobile devices that can be easily downloaded and installed.

IP Address
The Internet's version of a home address for your computer, it identify you when your computer communicates over the internet with other computers. It's how you navigate to others and others find you.

An Exploit
A malicious application or script that can be used to take advantage of a computer's vulnerability.

Breach
The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.

Firewall
Any piece of hardware or software that is designed to keep your data safe (i.e. behind a fireproof wall). It stops hackers connecting to your computer by blocking unauthorised access.

Malware
A term that describes any and all types of malicious software that is designed to penetrate and infect your device. Common forms include: viruses, Trojans, worms and ransomware.

Virus
A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others.

Ransomware
A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage until you pay criminals a ransom.

Virus
A piece of malware (see above) that often allows a hacker to gain remote access to a computer. It can sit and wait, undetected, for long periods of time before activating.

Phishing
A technique used by hackers to obtain sensitive information. For example, using fake email messages designed to trick people into giving-up personal, confidential data like passwords and bank account details.

THE END.

Information contained in this booklet has been obtained by Fidelity International from public sources. Care has been taken by the staff of Fidelity International in compilation of the data contained herein and in verification of its accuracy when published, however the content of this booklet could become inaccurate due to factors outside the control of Fidelity International and this booklet should, therefore, be used as a guide only.

This booklet is published and distributed on the basis that Fidelity International is not responsible for the results of any actions taken on the basis of information contained in this booklet nor for any error in or omission from this booklet. Fidelity International expressly disclaims all and any liability and responsibility to any person in respect of claims, losses or damage, either direct or consequential, arising out of or in relation to the use and reliance upon any information contained in this booklet. Fidelity International means FIL Limited and/or its subsidiaries.