Wakefield Central NPT

Neighbourhood News

From Your Local Neighbourhood Policing Team

WEST YORKSHIRE POLICE

neighbourhood policing teams npt

www.wypnpt.org

Cyber-safety tips

P@55w*rd5

Every site, device and application needs a password these days. They have to be so many characters long, not have a word from the dictionary, numbers, special characters and not be easy to guess but still be easy to remember.
Impossible, right?
Actually it's not as hard as you may think if you follow these easy steps:

- Pick some letters from the website you are using, for example Facebook – take Fc
- Think of a key word you will remember; E.g. Drive (backwards) evirD
- Add a special character or two; +!
- Finally tag on the total number of letters for the website/application; Facebook = 8
- Password: FcevirD+!8

As you can see, this is a very secure password which changes for each website but using this pattern is easy to remember. The above password will take about 1,600 years for a desktop computer to crack, as opposed to less time than it takes to make a cup of coffee if you use P@55w*rd.

Keep it private

Did you know that everything you do on the internet is monitored? Not by the Police or security services, but by your internet browser! Every website you visit, every search term you enter and every form you fill in is remembered by your browser. Whilst there are convenient reasons for this, the less information that you give the safer you are (and it could save you money too). On your browser go to the settings and look for "inprivate browsing" or "new incognito tab". Browsing in this way prevents cookies from being downloaded which means that every time you go to a site it thinks it's the first time that you've accessed that particular website so any special offers will still show, even if you've gone left the site to shop around. Try it the next time you book a holiday online, that special rate the first time you visited the site will still be there and not the slightly less special rate that appears the next time you go on the site.

Clear out your cache

Your devices store all sorts of information about you and what you do on it. Most of the time this is to save you some time when you go onto a website but do you really want this personal information, including your logon details, stored? Aside from the security risks this also slows your device down and takes up memory that could be used for a program that you're actually using at the time. It's always considered best practice to clear your cache data every time you switch off your device or close down a program. On your device search for "cache" and clear the data. Some devices and applications have a setting to do this automatically which will save you time.

Inside...

Neighbourhood News

AV or not AV? Not a difficult question.

These days we live off our mobile devices. Shopping, loyalty cards, bank details, contacts, login details, our location and so much more personal information is stored on our devices every second that it really does boggle the mind. So what are we doing to protect ourselves and our information? Most people will have an antivirus program on their computer or laptop but they won't have one for their mobile phone or tablet laptop, despite the fact that these are more powerful than the computers that put a man on the moon!!!

You don't have to pay an arm and a leg for a good antivirus, many of the free ones are just as good at keeping you, and your bank account and Facebook profile, safe from viruses and hackers.

A quick internet search for "free mobile antivirus" will bring up dozens of reviews and articles allowing you to pick the one that you like the look of to keep you safe.

Who says you can't get something for nothing?

Dodgy emails

Not a day goes by when dozens of new scams are logged by Police and cyber-security agencies in the UK alone. The one that may be familiar to most of us is the Nigerian lottery that we haven't entered but hackers and scammers are getting more and more creative and their emails look slicker and more legitimate with every passing week.

If you receive an email from your bank, service provider, utilities company, Windows, Apple, Google or anyone else telling you that you owe money or need to update your details through a link then chances are it may be a scam.

- Hover over the email address that it has come from, does it look legitimate?
- Who is it addressed to? Have they used your name and put your account details on there?
- Hover over any links, do they lead you to the correct website?
- If you believe that it is legitimate then navigate to the company website yourself without clicking the link and ring them

Keep up to date

Software updates, they're a pain aren't they?
Actually whilst they may be an inconvenience, especially if they require you to restart your device, they are absolutely crucial to keeping you safe.
Whilst some updates might have cosmetic changes such as a new layout or a new function, the vast majority are to fix flaws in the programming (often known as 'bugs') that hackers can exploit.
One bug on a popular social network simply required someone to type a certain string of code into the comments box and they got access to the users account. This bug has since been fixed, so long as you have updated the software/application for it.
On all app stores, all operating systems and all devices there is the option to automatically update applications and programs when a new version is available.
We recommend that you do this over WiFi to avoid potentially using loads of mobile data but a quick look through your settings (search for "update") on your app store and device should keep you safe with very little effort or inconvenience to yourself.

Contacts

Helpful websites

www.thinkuknow.co.uk

http://www.westyorkshire.police.uk/BlockTheWebMonsters

https://www.nspcc.org.uk/

https://www.getsafeonline.org/

https://www.o2.co.uk/nspcc