Wakefield Central NPT

Neighbourhood News

From Your Local Neighbourhood Policing Team

WEST YORKSHIRE POLICE

neighbourhood policing teams npt

www.wypnpt.org

Cyber-safety tips vol. 3

It looked like you….

Many new smartphones and other devices are using 'biometrics' as security measures. Fingerprints, iris scans, facial recognition even voice recognition are now touted as being big selling points for the latest gadgets. But how secure are these?

Facial recognition in particular is seen as being insecure. Using the shape of someone's face as the only barrier to gaining full access to your device is highly ill-advised as it's easily fooled. Even the latest versions which supposedly measure the depths of facial features like cheeks and eye sockets are still fairly easy to deceive.

Iris recognition and voice recognition are both slightly more secure but are still not considered the best form of security. As well as being hit and miss when you are trying to use them (try using a voice password in a car with the radio playing and three kids in the back) the most worrying thing is you're shouting your password at your phone in the middle of the street!!!
That's like standing at the cash machine shouting "Two! Three! One! Five!" As you put your PIN number in. Especially as the devices just go off how you pronounce the password and not what your voice actually sounds like.

Fingerprint technology on these devices has come a long way but nothing is as secure as a 6 digit PIN or a good, strong password.
For advice on how to create a strong password see Volume 1.

Back it up

What exactly is "The Cloud"?
Not the rainclouds, but "The Cloud" is remote storage for your information and data.
It's a backup of everything that you hold dear on your devices. Photos of the kids, holiday videos, documents and downloads, even which apps you've got downloaded.
Every single device will have access to cloud storage and best of all, most of it is free! You can pay for a premium service, or more storage, but for most of us the free versions should be plenty.

Manufacturers often offer their own cloud storage as well as many of the big companies that you probably already use (Microsoft, Google, Apple etc).
There will be easy to follow instructions in how to set these up, choose what you want to back up, how often and whether you want to do it over Wi-Fi (advisable so you don't run up a big bill).

All you have to do now is set a good password for your cloud service and even if something happens to your device, all of your important files are safe.

Who gave you permission?

All of our apps and services that we use have that annoying blurb about "wanting access" or "app permissions". Surely there's nothing wrong with blindly clicking "accept" all the time is there?
Actually, you may as well be signing a loan agreement without reading it.

A lot of these apps want access to your contacts, personal information, location data, passwords, gallery, camera, the list goes on!!!

Companies sell this information to make money, it's how Facebook makes $1bn a year despite being free.

You can manage these permissions in the settings for the app after you download them or alter them before you download the app. Does Snapchat really need to know where you are? Check the Snapmap feature to see why it might be a bad idea.

Inside...

Neighbourhood News

Down with the kids

How do you talk to your kids when they've been to the park or a club after school?
"Did you have a nice time? Score a goal? Who did you play with?"
That sounds about right doesn't it?

Now think about how you talk to them when they're online.
"What site are you on? Who is that?"
Bit more confrontational isn't it?
No wonder they don't talk to us about what they do online.
So what can we do to change it?

Put aside an hour or two a week to go online with your children. Bear with us here, this does make sense and it does work.
Let them show you what they do online. Little girl is into make-up blogs? Sit down and watch one with her, even if you are her dad. Son likes football tricks and wrestling? Put some time aside to watch the tutorials or highlights with him.

As well as spending quality time together, this gives you a chance to learn about their online lives. Trust me, no matter what you think, they'll have one.

Ask them to show you how they found the videos you're watching. Do they only watch them on this platform (like YouTube) or are they on iPlayer as well?
What about if they find something inappropriate that they don't want to see? Ask them how they would report it or flag it up.

Get them to show you how they would share it to their friends. Would they share it on Facebook? Who can see it? Can they upload their own videos onto YouTube and if so who can see them?
This isn't you being nosey, this is them teaching you about their world after all.

Remember that kids are encouraged to report their suspicions about people contacting them by everyone they meet. Police, teachers, group leaders, sports coaches, dance instructors and more all encourage **your** children to report inappropriate content and inappropriate contact.
When they do, please **don't overreact**. It is so easy to think "They're never going near the internet again" if they tell you about someone contacting them but this might be seen as punishing your child. Stay calm, let them know they've done the right thing and reinforce that this is why you take an active interest in their online world.

Never heard of that one before

Keeping up with the latest apps and games is like trying to ice-skate uphill sometimes.
So what hope do we have?

Well, if you have a good online relationship with your kids (see above) then they should be telling you which apps and sites they use. That's great but are these apps that you want them to use? Have you tried them out?

The NSPCC have an app checker which can be found at https://www.net-aware.org.uk/

Try typing the app into there or, if it's not on there, submit it to be checked.
In the meantime search the internet for the app or service. What do other parents have to say? What does the website say? Are there security and privacy settings that you can activate to make the accounts private?

If you don't like the app then discuss a suitable alternative with your child and explain why.

The trust has to run both ways but at the end of the day, **you** are the adult.

Contacts

Helpful websites

www.thinkuknow.co.uk

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

http://www.barclays.co.uk/ - Search "Digital Eagles"

https://www.getsafeonline.org/

https://www.net-aware.org.uk/