Dacorum U3A

Computer Support Group

30th October 2020

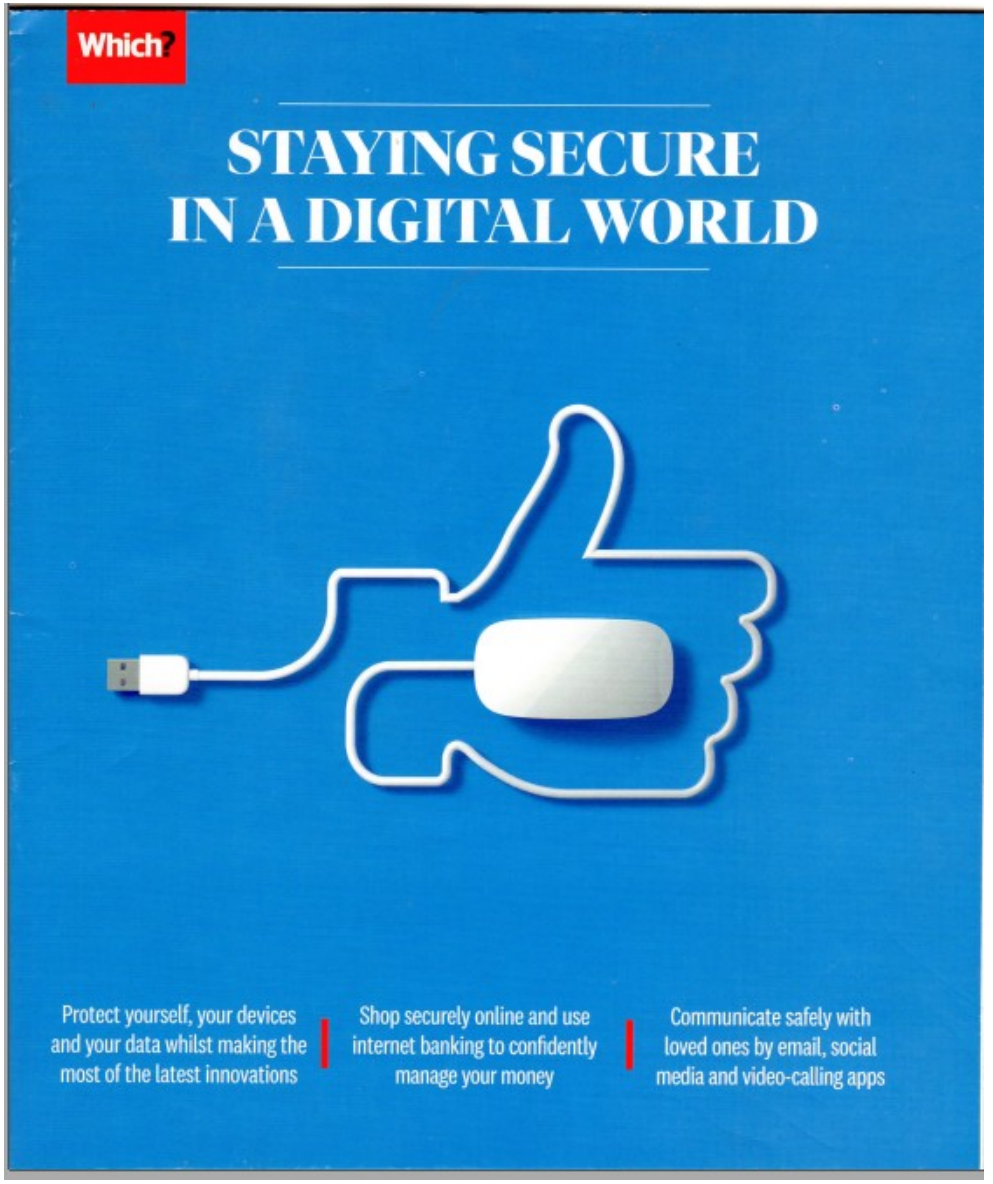
Agenda

- General discussion on the use of zoom
- Open forum
- Staying safe online presentation
- Tea and Coffee break (about 3.00 pm?)
- Continue Presentation
- Review of meeting

Staying safe online

This presentation is based on a Which? Leaflet.

It is not word for word but takes the essence of what Which is saying.



Contents

I will cover the following (not the same as Which)

- Two Factor Authorisation
- Defend your devices
- Antivirus
- Passwords
- Disposing tech
- Out and about
- Smart tech
- Email
- Social media
- Talking to others
- Banking
- Shopping

Two Factor Authorisation

Two-factor authorisation is designed to prevent unauthorized users from gaining access to an account with nothing more than a stolen password.

Two-factor authorisation is a combination of two of the following:

- Something you know (your password)
- Something you have (such as a text with a code sent to your smartphone or other device, or a smartphone authenticator app)
- Something you are (biometrics using your fingerprint, face, or retina)

2FA exposed

We are all familiar with the use of a password when logging on.

However, this is far from secure as it might be hacked or ‘key logged’. It is OK for things that don’t matter a great lot but is certainly not sufficient if money or important information may be compromised.

Several different methods are common but you, as a user, don’t have much of a choice.

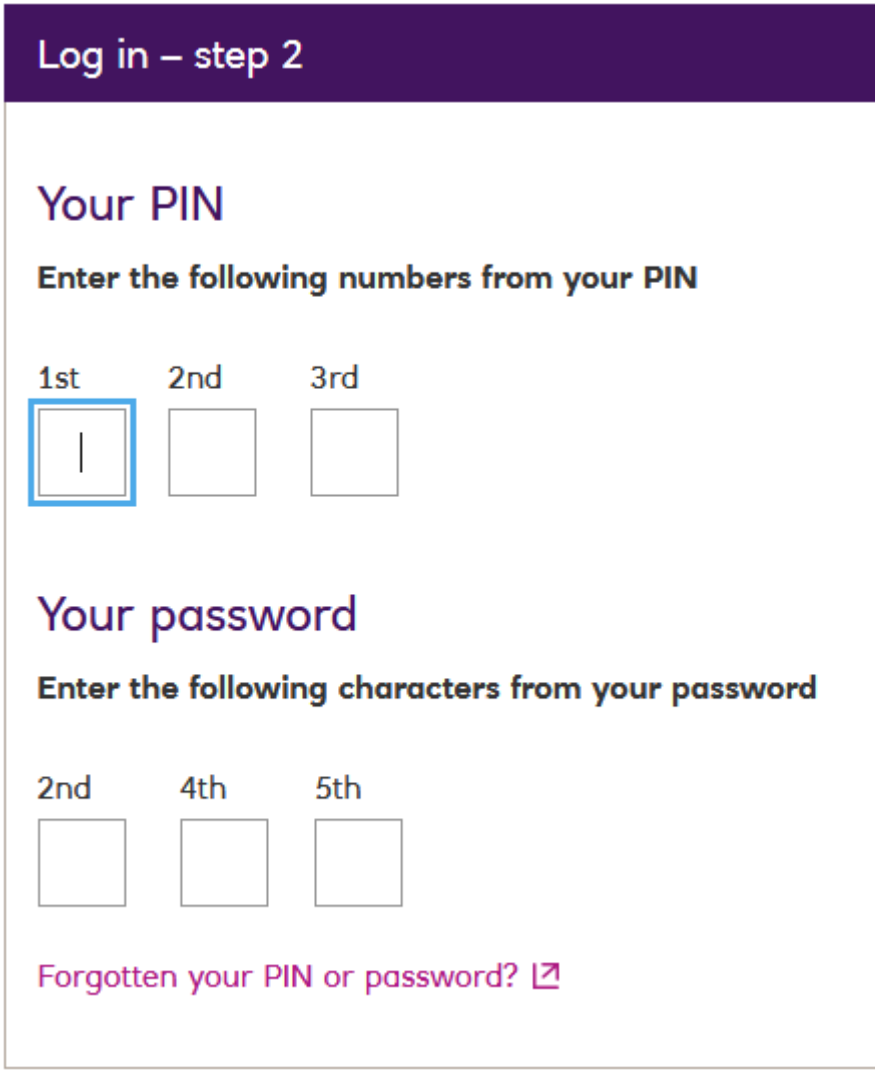
Some examples are:

2FA Using more than a password 1

This example from one of my NatWest accounts requires a variable part of the password. It also requires a part of the PIN.

Although it is not strictly 2FA as you have to ‘know’ both parts, it is better than just a password as it would take a long time for a key logger to be sure they have the full details.

Surprisingly NatWest came ‘top’ of the Which bank security list.



2FA Using more than a password 2

This method is almost certainly insufficient for many requirements (such as payments, card ordering etc.)

NatWest understands this and has a separate device for authorising these actions.

Despite this, I am surprised to see that NatWest came ‘top’ of the Which bank website security list.

Password updatable online. PIN updatable at an ATM?

2FA using a separate device 1

This shows a small (HSBC) device where the PIN is entered and checked. It is NOT connected to the internet so the PIN is ‘safe'. Instead a number is generated which IS sent to the Bank for checking.

At HSBC it is used along with a ‘modifiable’ user id and password.

It is used for tasks like authenticating logon and adding new payees. It could be used for making online debit payments.

The PIN in it cannot be changed without issuing a replacement device.

2FA using a separate device 2

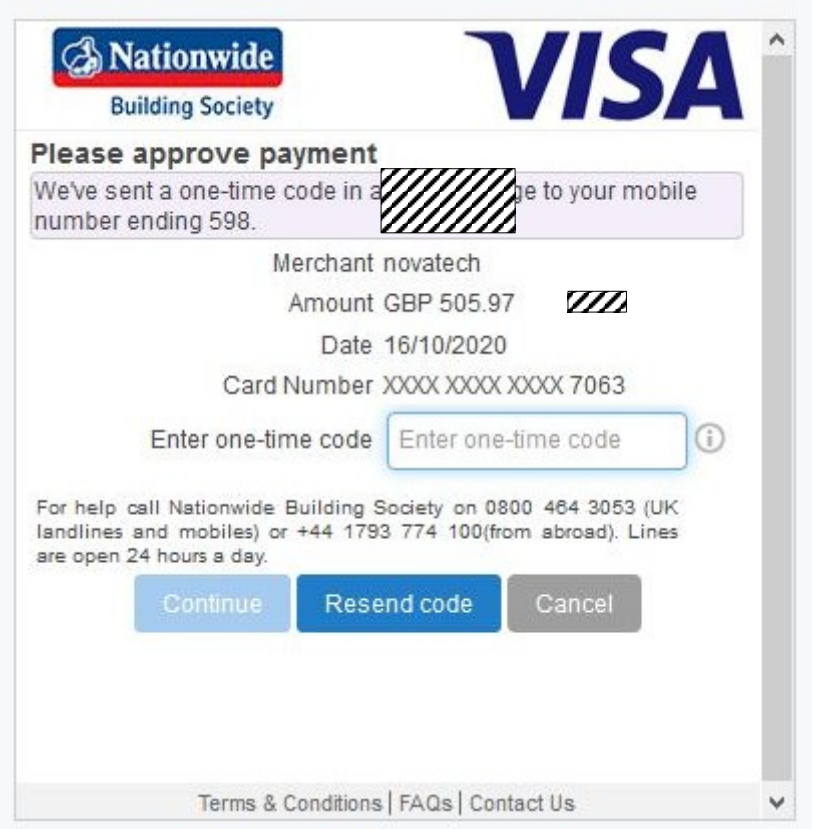
This is an example of a small device for checking a smart card. It is common to many Banks.

To use it a card is inserted into the slot and the PIN is entered. This PIN is sent to the card where it is checked. The PIN is not sent online but a number is generated which is sent to the Bank for checking.

The PIN in the card can be changed at an ATM. The number of invalid PIN retries can be reset at an ATM.

2FA using a telephone

- The system generates a number which it sends as a text to your (mobile) phone. You then enter this and the system checks it
- It is mainly used for purchases
- Here is an example of authorising a purchase
- It isn’t always purchases, HMRC uses this to confirm a login



Defend your devices

Software is regularly updated with security fixes. A virus checker is not really a substitute here

Updated software might not work on your device (Android is probably worse than the others)

Windows 7 has stopped getting security fixes so should be upgraded to Windows 10

Keep your operating system up to date if you can

With most connected systems you can locate them if they are lost

Defending against malware

It is obviously important to protect your devices against viruses and other malware.

Windows/Linux/Chrome PCs should have an antivirus system installed. Probably Windows defender is sufficient but there are many others

Apple PCs are generally more secure. However malware is increasingly being targeted here so an antivirus/malware system should be considered.

Apple phones and tablets are generally more secure and malware is rare on them

Android phones and tablets are better but malware can find its way in so an antivirus system should be considered.

Antivirus

As I said above it is vital to have good antivirus protection

Most free products work well enough, in fact, built in Windows Defender (and Firewall) work well enough

For Macs and mobile devices most of the main antivirus companies have versions for most devices.

The main difference between free and paid for antivirus systems are in the features and ease of operation

Passwords

The data you store is only as good as the password used to access it

Each login should have a separate password

However you can use the same password if the safety of the data is totally irrelevant to you

Don’t use single words but combinations of several unrelated words are OK e.g. treecakedog

Even better include upper case and numerics so: TreeCakeD0g. Even better still special characters so: Tree:Cake:D0g. Not all systems allows all special characters

Passwords 2

If you have to record the password, don’t just record the actual value but something related to it. E.g. T…:C…:D.. or OakSpongePet

There are password managers that will record the passwords for you. Personally I don’t but many people swear by them

Disposing tech

You probably don’t think about the data which is stored on your device when you get rid of it.

Although the data has been ‘deleted’, it is still there and can be recovered if you are expert enough.

The simplest way to logically delete all the data on a phone is to perform a ‘factory reset’. However, the data is still ‘there’.

On a PC, the similar action is a ‘format disk’. Note however that this will get rid of the operating as well. Again almost all the data will still be there.

Disposing tech 2

To completely and permanently erase the data a program must be used.

These programs exists for all the different tech you can find on the internet.

I use some facilities in Acronis. These allow either the permanent erasure of the ‘deleted data’ on a disk or the complete erasure of the disk.

These work by writing ‘0’s or random numbers to every location.

For physical disks they do this several times as it is possible to detect the contents of a location from its ’edges’.

Out and about

When you are out and about, it is tempting to use Public Wi-Fi. However, this can be quite dangerous as it is not that difficult for someone to ‘spy’ on the communication.

Any Wi-Fi that you don’t have to log in to with a password is likely to have this problem (and some that do).

Don’t access your Bank away from home unless you have your Bank’s banking app

Out and about 2

Make sure that your antivirus app AND firewall are both turned on

If you lose your iPhone you should be able to find it/lock it/wipe it, provided the feature is turned on. Ensure that “Send Last Location” is set as that will record where it was when the battery went flat. On another iPhone use the Find My iPhone app

If you lose your Android phone again you should be able to find it. Ensure that app is turned on. Go to android.com/find

Smart tech

Smart speakers, smart televisions etc. use the internet to work. This may use Wi-Fi or an Ethernet connection. We have to rely on the manufacturer for how secure the device actually is

Of particular concern are those devices that you can talk to. On most you can stop your commands being stored. You should note however that they continue listening for a time after you end your command

Using Wi-Fi is a perennial issue and you should ensure that your router has a ‘strong’ password.

On a smart television you should disable cookies and set privacy in the browser

Smart Tech 2

In the past some security cameras were found to have very weak security and could be used to talk to other devices on your local network.

Which has found that cameras using the CamHi app are particularly bad here, there are more than 100,000 of these check cameras in the UK

One of the issues here is that PCs tend to have less security imposed on messages from a ‘local’ device.

Smart Tech 3

You should:

Buy established brands

Always install updates

Set strong passwords (a password manager won't help)

Be careful what you agree to allow to be collected

Keep your voice controlled devices away from doors and windows so that they cannot be controlled from outside

If you receive security warnings: check the manufacturer's website

Be cautious if you see any unusual activity. It is best to unplug the device until you have investigated

Turn off devices if they are not being used

Talking to others

There are a plethora of systems that allow you to have ‘video’ calls over the internet.

Social media related systems are the ‘obvious choice’. However, the very social nature of the systems leave it open to scams and other problems.

Conferencing systems (like we are using now) are an alternative. They are usually free, but probably limit what you can do. However, if you want to talk to more than 2 people at a time,they are probably a better alternative.

The list given by Which doesn’t accord with my experience so I won’t repeat it here

Banking

On the face of it mobile banking appear to be less secure than using a Browser based. However, this is not necessarily true.

You have little real control over the software on your PC which could become updated when installing another piece of software. This should not be a problem if you get the app an official ‘store’.

For many banks 2FA helps here as it should be impossible for a hacked system to do anything serious when it is in use.

There are some advantages to mobile banking such as immediate freezing

Banking protecting against fraud

- Set strong passwords
- Protect media accounts
- Beware of phishing attempts
- Tell the bank if you think that you might have been a victim of fraud

Beware if anyone asks you for your login details, the bank will not ask you for these, however convincing a phone call/email might be

Attempted fraud should be reported to actionfraud.police.uk/reporting-fraud-and-cyber-crime

2FA security on mobiles

Some criminals are attempting to bypass 2FA on mobiles. They do this by trying to transfer the mobile number to their own phone.

If it works then the victim’s login codes may be sent to the fraudster.

Report 'sim-swap' frauds to your service provider if for example you get an email or text about your phone number being transferred (‘ported’)

Shopping online

- Beware of fake reviews
- Research before you buy
- Check the delivery costs
- Read the return policy
- Check if the seller is abroad
- Consider if the goods might be counterfeit

Smart phones can be used in a similar way to contactless cards but the £45 limit doesn't apply. You may have to enter a PIN or fingerprint etc.

Chargebacks apply to credit cards for purchases £100-£30,000

PayPal

The law and PayPal is a bit murky. If you use a card, in theory you are not paying the merchant. If you use your PayPal account you ‘might’ lose your chargeback rights. You might have to rely on the PayPal rules.

Some of the above applies to other market places

Confidentiality

Read the privacy rules of any site that might hold your personal data

By law you must be able to be ‘forgotten’

Note that, if you pay by card, the site might keep that card. Personally I try not to allow that

They will also have your name and address and probably an email address. These are vital parts of your identity, you have to trust the site where you give them

Summary

As I have said before:

Don’t Panic

Just Be Careful