Northern House School

Literacy News

SUMMER TERM, PART 1 018:30TH APRIL 2018

FOCUS THIS WEEK

DIGITAL LITERACY

Passwords

Privacy

Prevention

THINK U KNOW .co.uk

INSIDE THIS ISSUE:

Real Safety In A Virtual World

Thanks to the fantastic training this week delivered by the visiting **Murray Letham**, all Northern House staff and pupils are now aware of some of the complex issues involved in staying safe online.

Key to the presentation was the idea that we are our own biggest threat to our online safety, with our friends being the second most significant risk. So, for those going in with the idea that staying safe online was primarily concerned with issues of child protection, sexual exploitation and cyberbullying, there was a wet fish sized wake up slap around the face.

From internet enabled domestic devices to online banking, our lives contain countless ways in which we expose ourselves in the digital world. Our families, especially if there are young children, use technology in many ways every day, and for many of us our regular contact involves using some of the multitude of social interaction tools. It has become the social norm to message and to post and to not even think of the implications of inviting new technology into our lives.

The message from Murray was clear. There are far less real monsters in the world than we might think, but the risks to our safety and well-being are very real and present dangers if we do not remain aware and manage our behaviours.

This week we dedicate our literacy news to recalling some of the key points and suggesting simple solutions staff and pupils can use.

KEYWORDS

Adware: A malware to serve you adverts and monitor your use to target these ads.

Bot: Automated program. Unwanted bots run malicious code on the host machine, usually as part of a botnet (network of bots).

Cookie: A tiny piece of data stored on the device to remember information. Some cookies are essential as they remember your data and allow sites to function.

Drive-By Download: You visit a webpage that automatically downloads something nasty from the woodshed...

Keylogger: Never good. A program that records your key strokes, usually for malicious access to the device.

Malware: Generic term for programs designed to harvest data from you or your machine, usually for financial gain rather than malicious intent.

Ransomware: Such as *WannaCry*. Encrypts your device in the hope of you paying the ransom. Do not. Ever. Trash the device.

Scareware: Commonly encountered, will make you think your device has an issue and advise you to download a fix. Guess what...

Spyware: A malware, to monitor your activity.

Trojans, Worms & Viruses: All bad programs.

VPN: Virtual Private Network which allows you to encrypt data to keep your activities more private and secure.

Every Lesson A Literacy Lesson

NOW ON

The Summer Challenge

Stay Safe Online

Passwords

The internet of things is now with us. Any device that is capable of connecting to the internet, such as Smart TVs, toasters, heating and lighting systems, will have passwords. It should not remain on the default so you need to change it. If you don't, you risk being exposed but may never know if your device has been accessed remotely. For most devices, the default password is 0000.

Generally routers have unique passwords when new, so your wi-fi should be secure, but it is work checking. It is also important to visit the router webpage, and check that the admin password is set properly, or else you could lose control of your entire network , as the local address is always the same and this can be accessed from anywhere your wi-fi reaches, including outside your property. As an interesting aside, look at the available internet connections from your device at home and you will see just how far wi-fi reaches as you will see many connections in your area – some of which are always unsecured. Free wi-fi is never far away!

When thinking of passwords, remember they are the locks keeping you safe. Just as you have different levels of security on your doors, passwords need to be set appropriately. Simple ones are fine for sites where you are accessing their data rather than sharing your own but more complex ones will be used for email & social networks, with the most complex reserved for those sites covering your financial transactions.

Many security conscious sites now require 2 step verification for access from new devices or for new payment information. This means once you approve the access on the app or site, you will be contacted (usually by text or email) with a verification code to enter on the webpage. One downside to this is if you are logged in on your phone and the text comes to the same device, you have compromised your own security should your phone be lost.

Networks

Where possible, use wired connections as once you go wireless, your data is more at risk as it is floating around in the breeze.

Using a VPN, as you do when accessing the school server, means your data is encrypted, therefore more secure.

Most banks offer a program which you install in order to encrypt your online account access.

Where possible, access the secure version of the site, ie https://facebook.com not http://facebook.com.

Avoid signing in to your accounts from public or borrowed devices. Remember cookies? Even if you sign out, your data could still be on the device.

Check you have a secure password on your network. Some routers will allow you to provide a separate public access point to avoid you sharing your password with guests. Remember your wireless is available outside your property.

Links

Info

thinkuknow.co.uk

childline.org.uk

securingtomorrow.mcafree.com

getsafeonline.org

nspcc.org.uk

saferinternet.org.uk

safer-networking.org

Resources

lastpass.com

avast.com

avg.com

malwarebytes.com

meraki.cisco.com

Protection

Making passwords

Use a combination of letters, numbers and symbols for the best ones.

For the password reminder question, do not use answers other people could know. It is ok to lie in this case, so long as you remember.

Do not keep passwords on a sticky at the side of the screen. Nor on the desktop in an unsecured file. If you write them down, keep the record secure and if you have them digitally, password protect your file.

You would be unwise to use the same password for more than one site or service.

Remember if you sign into sites using another site account (my Facebook/Google/etc) that you are sharing your data across sites and allowing Facebook/Google/etc to harvest even more of your life!

There are free programs such as LastPass which make life very simple and secure. These auto create and store your account access details and allow you to create extremely secure passwords. Of course you then need to secure LastPass ultra-well.

Email

There are no limits to the number of free email accounts you can have, so make sure you have different accounts for different purposes and keep your main accounts spam free. Forwarding to your main account or programs like *Thunderbird* allow easy account management.

Devices

It can be difficult managing all the devices, when you consider PCs, laptops, tablets, phones and others, especially across a family. Some commercial device management software is free to use for non-commercial & home users. One fantastic resource is the Meraki Systems Manager from *Cisco*, which is user friendly enough for inexperienced users.

From the dashboard, you can monitor all your hardware, keeping an eye on storage and update status and access devices remotely. If you do run location services, you can also see where your devices are, so if they are lost/stolen you can find them, with options including erase the drive to prevent data loss.

All your devices should be password or code protected and backed up at least monthly, although getting into the habit of weekly scans, updates and backups is best practice. Make sure your backup is secure, on the cloud or other secure external drive. If your device is stolen it can be really annoying not to have that backup available. If you have space, keep the last 2 backups in case of corruption.

Update firmware, operating systems and protecting software—your device should be set to automatically check for and install updates for everything core, including these.

Anti-Stuff

You need to protect each device with antivirus, anti-malware and anti-spyware. You do not need to pay for these—those free ones are excellent, relying on being so good that users do purchase the upgrades. AVG or Avast are currently best for Antivirus. I recommend Avast as it has a number of other useful tools and less nag screens. To shield against malware, I use Malwarebytes as it remains reliable and warns against potential issues on webpages. Finally, run Spybot & CCCleaner. Both of these need to be set up to remove only the cookies and data you want to clean out, but it is well worth doing so in order to automate your device cleaning to keep yourself safe and your machine preforming at its best.

Siri

Apple users beware, for as the American say, Siri is a working girl and will go with pretty much anyone who talks to her. Your passcode is no defence against a silver tongue, for if Siri is listening anyone can launch apps on your iPhone. Indeed, if Siri is awake, anyone in the know can unlock your phone in about 3 seconds and enjoy full access to everything on there, including your money if you have the Apple payment app. If you don't need Siri, shut her down, as you should any app when you are not accessing it.

Old Accounts

We all make lots of accounts at sites we use briefly or occasionally. If you no longer use these, delete your account, and check that it is gone. Many sites allow you to 'disable' your account. This is not the same. Disabled means you cannot use it. But it is still there and so can be accessed and re-enabled. Deleted means it is gone. 'Delete and delete my data' should mean it also removes any activity linked with your account as it should cleanse the database of all your records, which is the best option if it is available.

Dear Deirdre

I forgot to turn on safe search when I installed a new browser and got some very nasty results. I mean I didn't even know it meant that now! I closed the page and tried to unsee it but I am worried I might have infected my computer. Please help. Delia, Norwich

You are right to be concerned as anything you access is downloaded to your machine so that you can see it. Delete your browser caches and your temporary files and you should be fine.

I am an adult and sometimes watch porn. It is just soft stuff and it is perfectly legal. I don't talk about it at work as I don't want them to think I am a pervert but I am worried if they find out I could be get sacked. Christian, Seattle

Your private life is just that and you are entirely right to not discuss some aspects at work. However, you do need to consider the implications when you work with children. Firstly, this must not be on any device you bring into school and you need to password protect the folder where it is stored if children access the device. If you are a parent, you need to ensure children cannot access the folder in order to safeguard them. If this does concern you, please make sure to talk to your union or the safeguard leads in school to ensure you are protecting yourself and others.

I had an inappropriate image come up on my laptop but deleted it so do I have anything to worry about? Mick, Whistable

Yes. Firstly, you should not have had access to such through the school filters, so if something did sneak in, please flag this with Watermans so they can update the filter. If a pupil searched using your laptop… Well, that's why we do not allow pupils to use staff machines!

Secondly, anything downloaded on your laptop is possibly still there. Deleting a file does not actually delete the file. It tells the machine the space in use by the file is available for reuse. To make sure it is gone, you would need to use a file shredder. If you do learn of this happening on any machine in school, please also report it so our techies can ensure it is cleaned out.