Supporting others to be safe online

Hello everyone, and welcome to today's talk for Cyber Safe Scotland week. Today, I'll be covering three important areas of how to stay safe online - **passwords, fake emails, and fake websites** – with a focus on how we as practitioners can help others stay secure, especially as the usual security advice can create barriers for disabled people.

Passwords

Passwords are everywhere. You need to use them for accessing your email; your banking; your amazon account; your social media, amongst many others. They keep potentially sensitive data safe: I might have sent a copy of my national insurance number via email to an employer. Passwords are also important because they confirm that you are 'you' online. If a fraudster had the password of any my shopping accounts, they could buy things using my card. If they had access to my email password, they could send emails to anyone they wanted. If they had access to my banking password, they could drain my funds, apply for a loan in my name, and drain that too!

At a basic level, passwords are important because they allow you to access services; access records of how you have interacted with services; and verify your identity online.

So how can we keep ourselves safe online? There are two aspects of password security that work together: strong passwords and unique passwords.

Strong passwords

Strong passwords are passwords that are difficult to guess. Although it's tempting to think that hackers try to guess your password, one attempt after another, it's much more advanced than this. Hackers use software to try passwords at a rate that a person can't match. Using a standard desktop hacking software can easily surpass 2.8 billion guesses per second. So, how can we keep ourselves one step ahead of hackers?

Consider the following when creating a password:

1. **Upper case letters**
2. **Lower case letters**
3. **Numbers**
4. **Special characters**
5. **Length**

Your password should be at least 9 characters long: the longer, the safer!

Many passwords have a minimum length of 8 characters, which would take just over 9 hours to crack – however, 9 characters would take 4 weeks; 10 characters would need 6 years.

6. **Un-obviousness**

Don't use things that are easily guessed, like special dates, names, places: for example, Aberdeen1! is a weak password, despite the fact that it complies with the above rules, because it could be easily guessed.

Unique passwords

However, strong passwords are only half the battle. To keep yourself safe, you must also use **unique** passwords.

A unique password is a password that is only used for one account. Using unique passwords means that if an account is compromised, then hackers won't be able to access other accounts.

The average internet user has over 200 accounts. This shows the importance of having unique passwords – using the same password for everything could give a hacker unfettered access to your life. However, it also illustrates the difficulty with password security: how can you remember 200 unique passwords?

Password Creation

Password generators can create strong, unique passwords instantly. For example:

KT8GxYqc=2@F

However, People with learning impairments, dyslexia, and low literacy skills might all find a generated password difficult to read and rewrite.

So, how can we balance the need for strong unique passwords with the barriers they can create?

Accessible password security

A secure way of keeping passwords safe is to use a **password safe**. Password safes are software that allow you to add account details such as usernames and passwords. They password protected, so this will keep your passwords safe in the event of a hacker gaining access to your computer.

Another way of keeping passwords safe is to write them down on paper and keep this in a safe place: it’s better to risk accounts being compromised in this way than to create weak, non-unique passwords to begin with.

The benefit of password safes is that you only need to remember one password to access the database you create. This password will of course need to be strong and unique. It also means that users can use a password generator to generate a password, and then copy and paste this into the password safe, and copy and paste from here when next needed. This helps overcome barriers for people with learning impairments and low literacy skills, because it removes the need to be able to read and rewrite the password. But how do we create strong, unique and memorable passwords to access the password safe?

Overcoming literacy or memory barriers for passwords

I think the solution to this barrier is to use a memorable short phrase or collections of words as a password. For example:

KeithElginForres15%
TheJungleBook88*

These passwords have the benefit of being strong, and the format can easily be adapted to make them personally meaningful.

For example, the first example is the first three stations heading north from

Huntly, but three memorable points on a journey can be tailored to an individual.

To ensure this meets all the requirements of creating a strong password, add a number and a special character on to the end. This pattern might be more easily guessed, but it strikes the balance between security and accessibility.

Fake emails

There are two types of fake email scam that we really need to be concerned about. Malware scams entice you to click a link, or download an attachment, and this can then infect your computer with a malware. Phishing involves a scammer sending emails to trick you into revealing your details. Closely related is the 419 scam, where a scammer promises you a substantial return, for minimal effort.

Malware

Malware emails often try and trick users into opening links and downloading documents. Accordingly, malware emails look innocuous – often purporting to come from legitimate companies or organisations, such as banks, local authorities, utility providers, credit card providers, and other big names such as Amazon.

Malware scams can also come from people saved in our contacts list if they have been a victim of a malware scam.

Phishing

Phishing emails often try and seduce us with an offer that is too good to be true, or worry us into giving details or making payments.

Phishing emails might claim to be from your bank warning you about suspected fraud, and asking you to move money into a secure holding account. Or, your energy provider explains that there has been an error with your bill, and you're either due a rebate, or else you owe them money. In these circumstances, pressure is often applied: **we have been trying to reach you, and this money will be written off/this debt will be passed onto the courts.**

419 scams are another type of phishing scam: you are contacted by someone who claims to be the agent of someone fabulously wealthy with a proposition for you. They have stashed £30m in a bank account during recent upheavals, but can now no longer access it without the UN confiscating it. However, **if you provide your bank details they can transfer this into your account, letting you keep a 10% cut of the money for your troubles**.

Or maybe you have been lucky enough to win the lottery, and **you simply need to pay a small administrative fee to access your winnings**.

How to recognise a scam email

The sender's address isn't right

Reputable companies usually register a domain. A domain is the part of the email address after the @. For example, the domain for my work email is **@lead.org.uk**.

If you have an email you aren't sure about, first hover your mouse over the sender's email address, and make a note of the sender's domain. Now, search for the actual company's email address: do they match? If not, then the email is likely to be spam.

Don't you know who I am!?

Is the email addressed to **you** (James MacDonald, Mrs. Miller), or does it have a generic opening like 'customer', 'Sir' or 'Madam'? Is this what has the sender called you previously?

Spelling mistakes

If you have received an email that has full of spelling mistakes, then it could be a scam: companies put lots of effort into appearing professional.

Links in the email look strange

Before you click on any links, hover the mouse over it. This should bring up the destination URL. Does this look right to you? If this looks strange – perhaps very long, or the domain looks wrong – this could well be spam.

The email is life changing

As the saying goes: if it seems too good to be true, it probably is. Many phishing and 419 scams promise you a vast sum for minimal effort – you can have £3m for letting someone put money in your bank account for a few days, or, for the payment of a modest fee you can access your winnings
These sorts of things don't happen in real life

You have been contacted at all

Some organisations, such as HMRC, will **never** contact you via email about fines, charges, and bills.

Accessible email security

Any of these should make you wary, and if two or more are present I suggest that you simply delete the email.

But just deleting emails can be difficult if you have anxiety, and finding spelling issues or peculiarities in domains can be difficult if you have learning impairments, dyslexia, or low levels of literacy. So how can we make email security more accessible?

If there is an email which seems like it might be suspicious, then the best thing to do is contact the organisation or person it claims to be from.

However, don't use any contact details that are present in the email. Search for the contact page of their website, and then phone or email them using these details. This means that if the email is fake, you won't simply be contacting the scammer. The organisation can then tell you if the email is fake and will be glad to know if their correspondence is causing concern.

Never open links or download attachments until you have done this.

Scam email avoidance

How can we avoid scams?

The first thing we can do is make sure our spam filters are turned on. While not perfect, using them can help catch fake emails before we have to worry about them.

The second thing we can do is keep our email addresses safe. This means not putting them online, for example in the personal information section on social media, and making sure that we tick “don’t share my data” boxes when filling in forms online.

Fake and fraudulent websites

Fraudulent websites are the website equivalent of phishing emails. Fraudulent websites try and trick you into entering sensitive information – especially card details. Fake websites are the website equivalent of malware emails. They might try and trick you into installing software that seems legitimate but is in fact some malware.

Pop-up scams

Some of the most common and convincing fake website scams are based on pop-ups which trick you into installing malware or making payments.

The IT support scam

The IT support scam starts with a pop-up, where you’re informed of suspicious activity on your computer, and told to call an IT technician on the phone number provided. However, when you phone, the scammer tricks you into giving them remote access, and “resolves” an “issue” they have found – for a fee. They may do nothing, and you pay for a worthless service. However, with remote access they can install malware.

Identifying fake and fraudulent websites

Is it secure?

When loading a website, look in the URL bar and see if the address starts with **https://** or **http://**. The **s** stands for **secure**, and this indicates that the websites uses encryption when transferring data. This encryption protects your data from hackers. Although **https://** doesn't guarantee security, it's a good start.

Does the domain look right?

Many fraudulent websites try and mimic the domain of legitimate companies, for example, tesc0.co.uk. Although these can be obvious if you're looking, if you aren't paying attention then it can be easily missed. It may also reference a brand, like www.nikediscount.com.

Don't click on links without first making sure the domain looks correct, by hovering your mouse over the link. If you're using Chrome, the URL will appear in the bottom left-hand corner.

How complete is the website?

Legitimate websites often have extra features on their site, like an 'about us' section, privacy policies, and shipping and returns information if it's a shopping site. Check these pages to make sure they are fully populated.

Most importantly, check the contact us page. Are there several ways of contacting the company?

How secure are payments?

Never buy anything online using non-refundable payment methods, like BACS. Make sure you use payment systems like card payments or paypal, as these both allow chargebacks.

However, chargebacks aren't legally required - they are part of a voluntary set of rules that banks sign up to, and if scammers have withdrawn money and closed accounts, chargebacks won't be successful.

You are better off just leaving a suspicious website than risking losing your money.

Is it too good to be true?

Are you being offered a new laptop for £100? Although you can get deals online which far exceed what you can get on the high street, if it seems too good to be true, it probably is.

Accessible website security

The advice here has similar accessibility issues as for fake emails: checking the domain can be difficult for people with learning impairments, dyslexia, and low literacy levels; and malicious pop-up scams can cause significant anxiety.

However, the best advice is to talk to someone you trust about your concerns. If there's still doubt, don't proceed. Fraudsters can cause irreparable damage, and this isn't worth an iPhone for £100.

With fake websites and pop-up scams, these can be managed by simply closing the programme, restarting your computer, and running your antivirus software.

Fake and fraudulent website avoidance

There are three practical steps you can take to avoid entering fake websites to begin with.

Antivirus Software

The first is to get antivirus software. This, like a spam filter, will flag up suspicious websites before you access them. As a good rule, if your antivirus software has flagged a website as malicious, don’t continue!

Keep programmes and systems updated

The second option is to make sure you update your programmes. Do this by turning your computer off when you have finished with it for the day, rather than leaving it on standby.

Disable pop-ups

The final option is to disable pop-ups. You can do this in your browser settings, and this reduces the risk of pop-up scams. Many websites need pop-ups enabled to access their full function, but you can whitelist them on an ad hoc basis.

Wrapping Up

So, we have looked at how we can make password, email, and website security more accessible. Passwords can be made more accessible by removing the cognitive load of remembering dozens of passwords by using a password safe, which only needs one password.

Email scams and website scams can be avoided by double checking that everything looks right. If there is still uncertainty, you lose nothing by asking - either the person the email claims to be from, or someone you trust, for advice - or by simply walking away.