www.onewest.co.uk

Please pass to your Senior Leadership Team & Data Protection Officer

Safer Internet Day 2021 is today (9th February).
Read our guide to help with tips that are relevant for everyone.

A message from Rob Long – Head of Information Assurance – One West

In my role heading up Information Assurance I am passionate about the need for Internet safety – it's amazing how vulnerable we can be even when we think we have things covered.

With my team in support of the day we have put together a brief bulletin covering the five key areas of internet safety – please circulate this to anyone you think relevant. Feel free to cut and paste!

1. Social Media
   - Don't always consider content as true and accurate – use **fact checking** sites such as https://fullfact.org/
   - Be **careful about what you post/share** – remember anything you post can be copied, shared or forwarded, and some employers look at social media profiles when recruiting.
   - Be **careful of giveaways, freebies & surveys** – they usually require you to share/like a post, and then go on to try and obtain personal information from you or infect your device with malicious software (malware). The blue check mark (on Facebook Profiles) gives you confidence the page is legitimate.
   - Make sure you **regularly check your Privacy Settings** (which are not always easy to find) and if **multi-factor authentication is available then use it** – this requires something else from just your username and password to login (such as a code sent as an SMS), and does not need technical knowledge and is an excellent protection.
2. Identity Theft
   - Scammers try and **obtain personal information from you**. Even your name (which can often indicate your sex) and age, along with your mobile number and/or email address is enough for them to **target you again** with posts/emails/SMS which are designed to draw you in to clicking and proceeding.
   - Don't throw away anything with your name, address, or financial information **without shredding it.**
   - Don't get tempted into posting/replying to posts on "20 random things you didn't know about me" - many of these are for **manipulating you into divulging confidential or personal information.**
3. Scams & Phishing
   - Unfortunately, during this pandemic, we have seen **an increase in attacks which use the current situation to their advantage.** Such as emails/SMS purporting to be from NHS (re Vaccines), Couriers (such as Hermes/DPD).
   - Rule #1- **Never click links or open attachments** on emails/SMS/DMs you were not expecting – most content will be developed to entice you to click (aka clickbait).

- Rule #2 - **Does the email look and feel right?**
  - Does it have poor spelling/grammar?
  - Does is address you by name? (and not Dear Customer)
  - Look at the sender's email address – does it look right? (often a slight spelling mistake is there to trick the eyes, e.g. info@nati0nwide.com)

4. Cyber Bullying

Young people

- You may feel scared, ashamed, or afraid to flag something to your parents or teacher - **make sure you tell someone**

Parents

- **Be available for your child to talk to you** about their worries and make sure they know where they can go to for support.
- As children spend more time online, they can be exposed to more advertising that may promote unhealthy foods, gender stereotypes or age-inappropriate material. **Help them recognise online ads and discuss together** what is wrong with some of the negative messaging you see.

5. Obscenity & Grooming

- Ensure you have **web filtering in place** with your broadband provider – most have made this easy to setup/configure.
- Be really careful and **not trust people online** if you can't be sure who they are.
- Ensure you have **a culture of openness with your children** to allow them to talk openly about online behaviour - how they behave online, and how other behave online.
- **Look out for the signs -** often groomers will:
  - Send you lots of messages
  - Ask you to keep things a secret
  - Start sending you sexual messages
  - Get you to share personal information
  - Try to blackmail you

Other helpful resources:

https://www.saferinternet.org.uk/
https://www.actionfraud.police.uk/
https://www.ceop.police.uk/safety-centre/
https://www.childline.org.uk/

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

I hope this proves useful!

Kind regards

Rob Long

Rob Long
Head of Information Assurance
One West