Thank you for coming to the 'Communitech' Workshop!

Thanks for taking part in our workshop, we hope you learned something about being safe online!

We have listed some of the important information you should remember from today. You can also share this information with family friends, so they can be safer online too.

The Value of Personal Information

Personal information, such as where you live or your favourite food, is valuable. This information tells people something about you, for criminals it tells them something that they might be able to use against you.

A criminal might be able to use your personal information to work out what your passwords are. They also might be able to use the information to create convincing scam emails, known as phishing emails, to trick you.

Remember:

- Try not to share your personal information online
- Make sure your social media accounts can only be seen by your friends
- Don't add people you don't know

Be Careful When You Use the Internet in Public

Be careful when you connect to the internet in a public place, it might not be safe and could have a criminal using it. They will be able to see what you are doing on your device while you are connected to the same WiFi as them.

Make Sure the Apps You Download Are Safe

There are so many apps you could download, it can be difficult to know which ones are safe. You should always be careful when you are choosing which app you would like to put onto your device because if it has been made by a criminal, they will be able to see what you do on your device.

Only download apps that have lots of good reviews. Make sure that the review goes back a long time too. Sometimes criminals will put reviews on their apps so people think they are safe when they're actually not.

Watch Out for Online Quizzes and Games

Some of the games and quizzes online, like ones on Facebook, are safe. However, some are not. If you are ever taking part in a quiz or game that asks for any personal information, do not give it.

Communitech Workshop

If an Offer Seems too Good to be True, it Probably is

If you receive an amazing offer through your email or your social media accounts, be careful. It could be a trick to try to get you to click on something with viruses or get you to give out your personal information, such as your bank details.

Offering something amazing in return for something little is a common trick used by criminals online, if you or someone you know is offered something like this just delete it so you aren't tempted by it.

Be Aware of the Latest Online Threats

It's important you know the latest tricks used by criminals online. You can find them out by searching online about them.

One of the latest threats is the use of fake QR codes, these codes send you to a dangerous website that the cybercriminal has made, so it will probably have lots of viruses on it or ask you for some personal information. Always be careful when any site asks you for information about you or someone you know.

Downloading Games and Films Can be Dangerous

It might seem like a great idea at the time, but downloading games and films from websites instead of paying for the real one can be dangerous. Criminals online know that people want to play new games or watch the latest films, that's why they create websites that offer them for free. But what they do is attach viruses to the file that you download.

Only Use Safe Sites

When you are online, only use sites that have a padlock next to the website address, and make sure the website address starts the "https". If a website doesn't have "https" it means it is a dangerous website.

Some criminals create websites that start with "https", if you are on a site that has this at the start of the website address, but it asks you to download something or give out personal information, it could still be dangerous,

Use Strong Passwords

For passwords to be strong and secure they can't be made using information about you or someone you know. Personal information can be found out, and this means that passwords using the same information can be found out too.

Your passwords should be made using three random words, like: 3BirdsTwoTrees