SPECIAL EDITION

Latest News from SeniorNet Cambridge

Editor: Email: las_palmas2002@hotmail.com

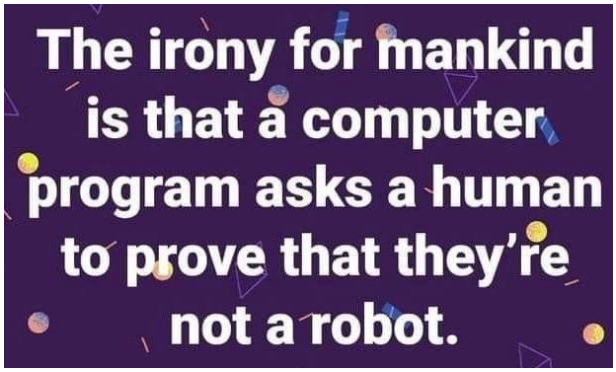
ISSUE No. 114. November, 2021

Feedback: mailto: cambridge.seniornet@gmail.com

Editorial

This newsletter will be briefer than normal. Although we have had slight reprieve this week, the continuing restraints of Covid have severely restricted our activities. Even with further liberation, it is highly unlikely that the Health and Community Centre would permit us to have a gathering of up to 100, so your committee have reluctantly decided to cancel the November Social Meeting. So no Xmas lunch this year. Covid is definitely the Grinch who is trying to steal Xmas! We will let you know of any other developments by email.

Malcolm



ATexan farmer goes to Australia for a vacation and while he's there he meets an Aussie farmer, They get talking and the Aussie shows off his big wheatfield. The Texan is unimpressed, saying "We have wheat fields that are at least twice the size of that" They walk around a little more and the Aussie shows off his herd of cattle. The Texan is again unimpressed and says "We have

Longhorns that are at least twice as large as your cows. After walking a little further the Texan spies a group of kangaroos hopping through the field. He says to the Aussie "And what are those?" The Aussie replies " Don't you have any grasshoppers in Texas?"

****

CYBERSECURITY AWARENESS MONTH

October is designated as 'Cybersecurity Awareness Month'. Just like Covid 19 which seems to be everywhere and continually creating problems for all of us, cyber criminals are out there and very active and especially in this Covid climate. Knowing how they operate will help us be aware and constantly on alert to protect ourselves.

The following information was adapted from a Cyber Security Newsletter.

Cybersecurity awareness month: Fight the phish!

Phishing crooks get to try over and over again. **But you only need to make one mistake...**

In general, there are four main steps phishers go through when creating convincing phishing emails, and understanding these steps helps you to spot and stop them.

Step 1: They pick their target. Different people fall for different tricks, so the more information they have about their target the easier it is to craft a convincing phishing lure.

The audience may be broad, for example users of a particular bank or people who need to do a tax return, or it may be very specific – such as a particular role within an organization or even a specific individual. Either way, they always have an audience in mind for each attack.

Step 2: They choose emotional triggers (select the bait)

Attackers play on our emotions in order to get us to fall for their scams. Here are three emotional triggers that phishers commonly exploit to trap you – sometimes using them in combination to boost their chance of success:

- Curiosity. Humans are naturally inquisitive and phishers abuse this by making you want to know more. All you need to do is to click the link or open the attachment…
- Hope. The abuse of hope by phishers can range from general messages about unexpected prize wins and dating opportunities to specific emails referring to job offers, pay increases and more.
- Necessity. Phishers often use a cybersecurity lure – pretending that you've suffered a security breach – to make it sound as though you simply ***must*** act now. This phish tells you that you need to change your password or else…

Step 3: They build the email (bait the hook)

Next up, they need to build the email. They will often attempt to cloud your judgement.

For example, an attacker might send you an email that appears to contain clickable links to weight loss products. At the bottom of that same email, the attacker also includes a clickable "unsubscribe" link. Here's the catch though: clicking on the "unsubscribe" link takes you to the exact same place as clicking any other link in the email. **Never use the 'unsubscribe' link if you didn't subscribe originally.**

This way, the attacker presents you with the illusion of a choice while ensuring they get you to click the link they wanted, regardless of where in the email you do it.

Step 4: Send the email (cast the line)

Finally, the phishing email needs to be delivered to the targets. There are a variety of ways for an attacker to do this. They may simply create a new email account on a generic service like Gmail and send the message using that email address, or they could be a bit trickier about it.

Attackers sometimes purchase unregistered domain names that look similar to a legitimate domain, changing the spelling slightly in a way that isn't obvious.

They will then send the phishing email using this lookalike domain in the hope that **users *who are in a hurry*** won't spot the subtle difference.

It's also possible for attackers to compromise an email account that belongs to a legitimate source and use it to send a scam message.

Even if a phishing email does reach your inbox, it still requires you to take some specific action – clicking a link or opening an attachment – before it can succeed. **One of the best protections is your own common sense.**

STOP, THINK, BEFORE YOU ACT.

Stay safe online and happy computing.

Muriel

Some Federation support  **partners**