Dacorum U3A

Computer Support Group

31st May 2020

Agenda

- General discussion on the use of zoom
- Open forum
- Personal Privacy presentation
- Tea and Coffee break (about 3.00 pm?)
- Continue Presentation
- Review of meeting

Personal Privacy

This presentation will look at various aspects of ensuring that, as far as possible, you keep yourselves Private and help stop fraud.

- Emails
- Online Purchases
- Social Media
- Smart devices
- Smart Speaker/Television

What is Privacy

Dictionary definition:

- the state of being apart from other people or concealed from their view; solitude; seclusion.
- the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone.
- freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one’s personal data or information, as by a government, corporation, or individual: Ordinary citizens have a qualified right to privacy.
- the state of being concealed; secrecy:

Privacy GDPR

The GDPR aims primarily to give control to individuals over their personal data.

Personal data is information that relates to an identified or identifiable individual

The GDPR applies to processors outside of the European Economic Area (EEA) if they are engaged in the "offering of goods or services" (regardless of whether a payment is required) to data subjects within the EEA, or are monitoring the behaviour of data subjects within the EEA

Email

Most people have only a single email address that they use for all purposes. If this email address is compromised, it is a lot of work to start using a new one.

Personally, I have an address for my personal communications and a separate one for purchasing.

Most Internet System Providers (ISPs) allow their users to have more than one email address.

Multiple Email Addresses

Having multiple addresses can complicate things.

The ISP's online system will usually only access a single email address at a time. This would mean regularly logging on to each email address separately.

The solution to this is to use an 'email client' to give access to multiple email addresses simultaneously. I use Thunderbird and have 12!

There are other email clients, including some specialised ones for smart phones.

Email Hacking

Up until recently, many email systems were not encrypted. This potentially allows ‘people’ to see your emails.

Another potential problem with emails is that the address book can be ‘hacked’ if your virus protection is not very good. (Note here that no virus protection can be perfect).

Hacked address books

If your address book is hacked then the hacker can send out emails purporting to come from you. You might treat such a message with less diligence.

Here is an email I received from a friend:

EM

https://bit.ly/2ZgASvi

It is fairly obvious that it is suspect but difficult to see what it really is. In fact it resolves to:

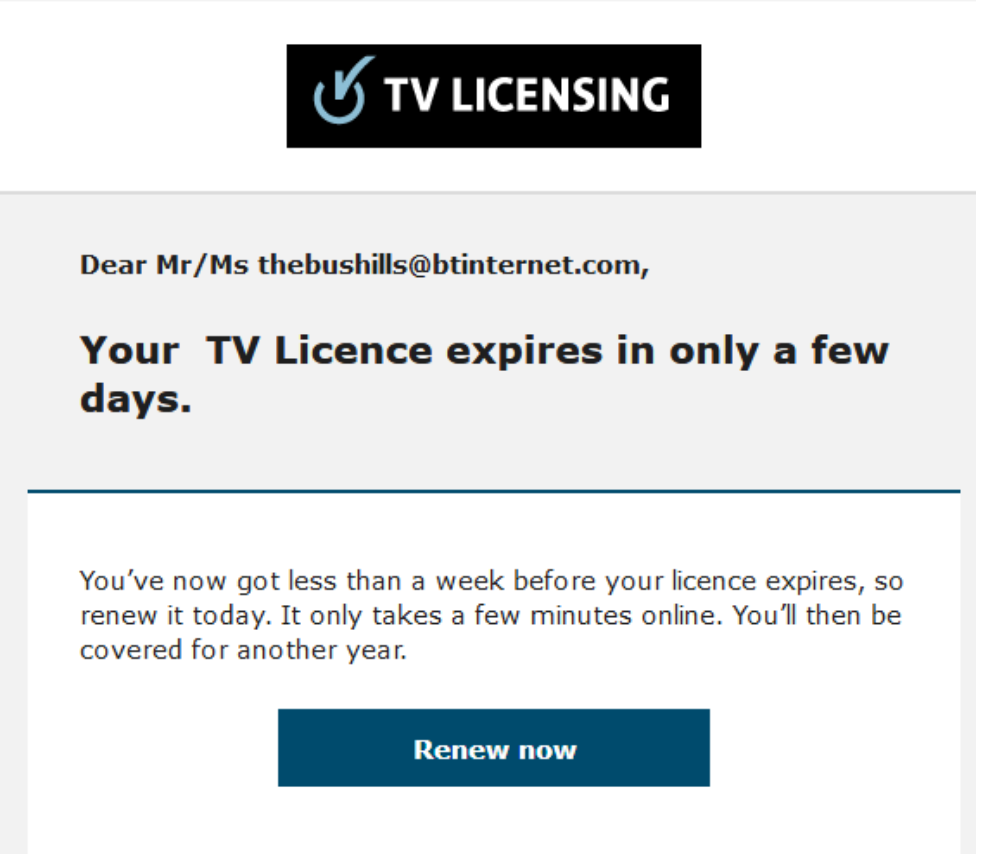
http://alloy-insurance.com/.well-known/pki-validation/subscribed/articles/blogger/url-log.php/quc/xwy/?material=11ynp2cp00ngvm

goo.gle is a similar ‘URL shortening’ facility.

Email Phishing

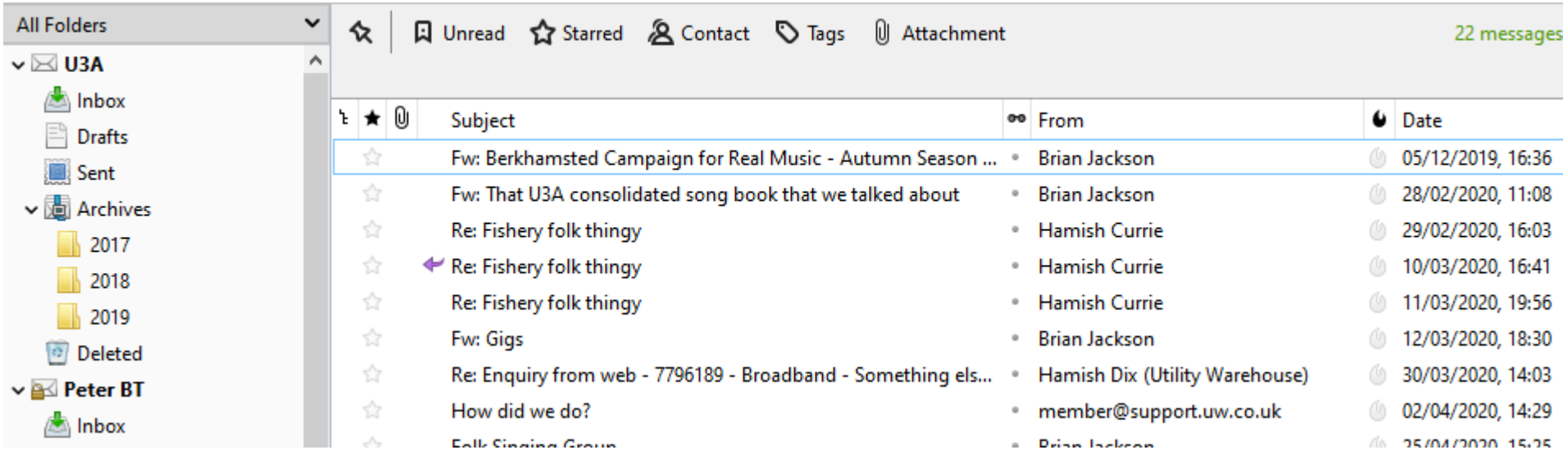
A phishing attack is where you are sent an email looking as if it has come from a legitimate source. With a link that will request your various information and including perhaps account information.

In this case, the renew button starts a page in hsedu.vn. Obviously NOT tv licensing.



https://hsedu.vn/.home/cpc77.php

Thunderbird



The above is an example of some of my addresses (Peter BT is actually 2 addresses).

The bottom of the screen shows the content of the email.

Because all of the data is ‘local’ access is almost instant.

Online Purchases

There are obvious risks when making purchases online

Never agree to transfer money to the merchant's account directly. You have no control over who the merchant really is and whether the account number is correct.

It should go without saying that you should only make payments using a Secure Site – 'https:..'. This should ensure that only you and the merchant you are using will be able to see your card details.

Online payment by Credit Card

For Credit cards only Section 75 gives you rights to claim back from your card issuer for purchases between £100 and £30,000.

This protection applies only to single items but includes partial payments (e.g. deposit).

Outside of these limits (including Debit cards) you can still make a ‘Chargeback’

There are doubts as to whether this applies to additional cardholders. So to get the full advantages the main cardholder should make the major purchases.

Online payment by Card

Chargeback allows the you to make a claim against the Merchant's bank for the following sort of reasons:

If you do not get the goods or services you paid for, including If the company has gone out of business

If goods or services turned out to be faulty, counterfeit or defective (you will need to return the goods in order to get a refund in this case)

If you are charged the wrong amount, or charged twice by mistake

If you are charged for a repeat payment after cancelling a subscription.

Online payment by card

You have to enter sufficient information about your card in order to make a purchase. The merchant might want you to set up an account with them and store this card information.

It is best not to allow this storing as, if the merchant gets hacked, more payments can be made.

This is not as bad as it might seem as if the item is to be delivered, the address would be wrong and if the billing address was changed it would no longer match the card address.

Paypal

If you use Paypal the position if far more murky to pay, using your card:

There are arguments that having another party involved in the process takes away the Section 75 protection.

PayPal also offers its own buyer protection scheme, called PayPal Buyer Protection, so it's worth checking if you'd be covered by that if you have a problem with your purchase.

If you particularly want to have the protection of Section 75 then try to pay the trader direct with your card.

Online purchases address

It is almost certain that you will have to provide a ‘billing address’. This allows the card company to check that the address is pukka.

If this is an electronic download this is the only address they have so it is difficult to confirm.

They will usually ask for a ‘delivery address’. They should ask for extra checks if this is different from the ‘billing address’.

Online purchases name and email

The merchant will probably ask for a name and an email.

The name is largely irrelevant as it is only used for communication. However, the ‘name on card’ is required so that the card issuer can use it to check the transaction.

The email should be a valid one that you look at but it probably shouldn’t be the one that you use for personal communications. If you use a separate one then make sure that you check it from time to time. An email client helps here.

Purchases ‘Buy now pay later”

There are various online systems that allow purchasing without a card.

There is sometimes little or no check on the information given.

Which says that Klarna is apparently particularly bad here. They require various personal information, most of which is fairly easily available online. It may therefore be relatively easy to clone someone’s identity, even if only for a single purchase.

Social Media

Using social media has a huge potential to compromise your private information.

Some of this is not obvious, e.g. a 70th birthday party on a particular date immediately exposes your date of birth.

A year or 2 ago Which did an article where enough details of 3 or 4 people could be gleaned to enable their identity to be cloned.

Even a picture can be used to show that you are not at home.

Social media safety

It is therefore VITAL that you limit the people that can see anything other than the most trivial.

This advice extends to the people who you do allow to see your information. You must ensure that they do not forward anything, unless you tell them otherwise.

Smart Devices

Almost by definition, Smart Devices are connected to the Internet. This is almost certainly done using wi-fi to your local network.

This is a potential problem as, once into the network, there is very little checking. Therefore, in theory the device could access any computers also attached to that network.

Even with high quality devices, security updates are only provided for a very limited period.

There are extensions available for some computer that allow fine control over the ability of these devices to access them.

Smart Device Password

It is vital to change the password on the device, otherwise someone in the street or across the Internet could get access to the device. They could then change it, possibly install new software. They might view your camera or change your heating or open your curtains!

Your router will also have an admin and a wi-fi password and although these may be a random one, it is probably a good idea to change them (don’t forget to change it in your laptop etc)! The router is usually accessible using address 168.134.1.1 in your browser.

Smart Speakers/Televisions

An additional problem relates to Smart Speakers and Televisions: they have access to your preferences.

They also have your email address.

They can then transmit the information centrally.

This combination allows targeted advertising

Smart Speakers

There is an extra problem with Smart Speakers. Unless they are turned off, they listen to what is being said within range and send it over the Internet.

The information is then recorded and ‘a small sample’ is listened to by the staff.

This is sufficiently a problem that at least one of the (I think Google) executives makes sure that the speaker is turned off before having any important discussions.

Summary

Don’t Panic!

Just Be Careful