Security

Security (ComTech ASDA 29/01/2026)

- For this presentation we'll describe this as a discussion on steps to prevent or mitigate threats to your data, your finances and/or your person, arising from events or malign access to one of your devices.
- … so it won't cover other security issues.

- It will refer to (but not overlap with) with topics to be presented by Peter H in the next session on 'Backup' – key and essential part of your security planning.

Security

- So here is our u3a member at his PC / using his device . If not connected to the internet, is his data secure?

Security

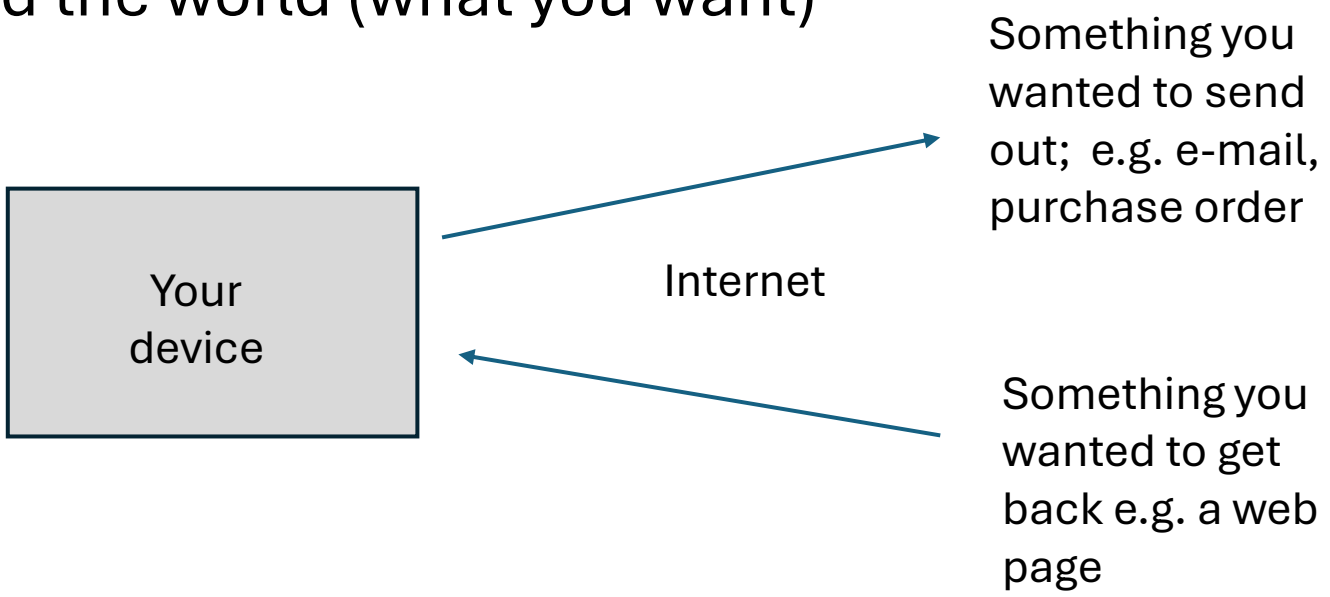
- So here is our u3a member at his PC / using his device . If not connected to the internet, is his data secure?

Security

- No, there is a whole range of threats which might affect him
  - Machine failure
  - Fire
  - Accident
  - Theft
  - Dog urine
  - Deleting data by mistake
- The detrimental effects include
  - Loss of key data (and replacement costs thereof)
  - Loss of hardware
  - i.e. money, time, reputation

Security

- You and the world (what you want)



Security

- You are connected to a global network

Your device

Something you wanted to send out; e.g. e-mail, purchase order

Something you wanted to get back e.g. a web page

Direct physical access to devices e.g. thief, man in repair shop etc.

100m hackers

People who would also like to have access to your device for malign purposes

Security – basic fundamental approach

- *The effort put into security should reflect the value (and ipso facto the cost of loss / damage) of the data accessed or lost. More or less is sub-optimal.*

- For many of the scenarios here, the key mitigation is to restore from a backup. [If you never do one, you will after losing your wedding / grand children's photos or re-typing 50 pages of lost data]

- Peter will explain how to minimize loss in his session!

Security – additional (and subtle) considerations

- These overlap with Peter (which I'm sure he will cover), but if these situations apply to you, take care
- *"I'm safe because I use One Drive / Google drive and back up to the cloud"*
- *"I do a daily weekly / monthly (whatever) backup and can't lose anything"*
- Both can be wrong. The subtle reason is that there is a difference between a 'backup' which saves a copy of the then current state of your device, and an 'archive' which preserves a historical record of your data.
- These services often also use something called 2 way sync, which is the spawn of the devil
- If you have important data on your machine, understanding this is important! Peter will explain!

Security – example scenarios

- Scenario 0 : You don't have an up-to-date anti-virus package on you machine (Windows defender is ok)
  - Oh dear … one of the 100m hackers may well get you.
- You are familiar with most of the weak points, with attack via e-mail/web being at the top of the list
- Never
  - Download a file when you are not sure of the source
  - If you do download, do a virus scan on it before use
  - Always check an email's sender; Something supposedly from Bristish Gas with a sender address of sergei1251@hackersquad.ru isn't
  - It's a good idea to examine the raw message if there is a button to click (more on this if required)

Security – example scenarios

- Scenario 1 : No material personal data on device; however, If data were lost, you would wish to restore them.
  - Prevention: steps to physically protect device; limit invited access (e.g. external agent support)
  - Mitigation : restore data from backup (you have one, of course?) and you are back to normal.
  - Nerd note, which Peter may cover
  - If your device main storage gets corrupted, it may not start properly, and a normal backup probably won't help. The approach here is to do what's called an 'image copy' or 'block copy', witch in conjunction with a 'recovery kit' can probably re-instate the system. Peter has proposed we look at ways to do this with all u3a used machines. In most cases it's a bit too technical for most users.

Security – example scenarios

- Scenario 2 : You use an e-mail client like Outlook and keep copies of utility bills on the device.
- Scenario 3 : You keep substantial amounts of personal and/or financial information on the machine.
- Scenario 4 : You are a u3a Trustee and you keep accounting of regulatory materials on their machine with no other copy.

- Here we need to look at the risks from having such information potentially exposed

Security – example scenarios; the risks

- I'm not covering issue which can be fixed by properly designed backup (and where relevant, archive) procedures.
- The non-backup risks are primarily the result of unauthorized access to the device – discussed in what follows.
- Example Risk 1: The machine goes for repair. Here you take the machine to Curry's and grant access to the 17 year old assigned to look at it. Alternatively, you allow remote access to it by, say 'Which Tech Support'.
- By default these staff can see all the information. This risk arises from possible personation

Security (non exhaustive)

- Risk 1 (cont) : This risk arises from possible personation by the person with access or a third party to whom it is passed. What data is there? Could a bank or other organization be convinced by an assumed identity?
  - **Risk 1 has a huge potential financial hit**
- Risk 2 : is there any information that might be used for blackmail or reputational harm?
- Risk 3: Cold a third party have installed a ‘keylogger’ (copies you keystrokes and sends them to the internet, including your bank passwords
  - **Risk 3 has a huge potential financial hit**

Security – one contributing solution

- Encryption. This is when your important data are ‘scrambled’ and can only be accessed if you enable that with a password. This deals with the unauthorized aces issue (but not a keylogger).
- Both windows and Mac have facilities to do this, but note
  - Win 11 Home 2 points
  - Win 11 Pro 4 , 7 or 8 points
  - Mac 9 points
- Windows drawbacks can be dealt with by using third party products.
- Happy to provide more information or delve into this at another time.

Security – device and other issues

- The following issues can lead to a serious breach or just be a major PITA.
- Two Factor Authorization: If you use your phone for this, have you a strategy for action if you lose it? (Tried to speak to a human at the bank recently?) (Maybe a cheapo Nokia also registered with the bank?)
- Password vault: You have got one of course. But if the machine gets stolen and passwords are held locally on that machine have you a separate independent (and encrypted) copy? Or can you actually remember 50+ passwords of the type ‘REWGFnsvsnjh%%4176” (Or maybe you use ‘Fido’ for everything?)

Some ChatGPT tips

ChatGPT tips – making AI work usefully

- The current AI hype has generated a whole spectrum of reactions from experts and the general public alike. (“hallucinates” “will take over the world”)
- A more measured approach might be that it is incredibly useful for performing the sort of tasks for which it is applicable. (It’s good at what it’s good at)
- This section has a few thoughts to share about its applicability I’ve had from my usage (including that it is very good at solving computer and security problems)
- Its use extends beyond using it as a more friendly Google or improving holiday snap.

ChatGPT tips – making AI work usefully

- Is it intelligent?
  - Yes, in that it can arguably pass the Turing Test (1950) and beat a chess world champion (Kasparov)
  - No, in the sense that, as the ‘T’ in GPT indicates, it has been ‘trained’ on a vast repository of knowledge which it can re-assemble to answer questions; mind blowing programming, but it lacks the human capability for such things as questioning axioms, for example – it does not ‘reason’ in the human sense. Kasparov could still beat it, if push came to shove

ChatGPT tips – making AI work usefully

- Is it intelligent?
  - Yes, in that it can arguably pass the Turing Test (1950) and beat a chess world champion (Kasparov)
  - No, in the sense that, as the ‘T’ in GPT indicates, it has been ‘trained’ on a vast repository of knowledge which it can re-assemble to answer questions; mind blowing programming, but it lacks the human capability for such things as questioning axioms, for example – it does not ‘reason’ in the human sense. Kasparov could still beat it, if push came to shove

ChatGPT tips – the importance of the ‘T’

- GPT doesn't reason. It recovers and reassembles data it has.
- So it works well as a ‘super Google’
- This is why “would “Bingo Technologies be a good buy for my pension” is a slightly dumb question.
  - It doesn’t know what your investment criteria are
  - It can no more forecast the future than you can

- *Special note : ChatGPT Pro can keep a history of all interactions AND you can ‘train’ it with you own personal data. It’s therefore leaning about YOU. With the pro version you can build personal GPTs.*

ChatGPT tips – issue 1 : context

- People generally ask questions in the framework of some unspoken context. GPT has no context at all and applies it processing to just the query in isolation.

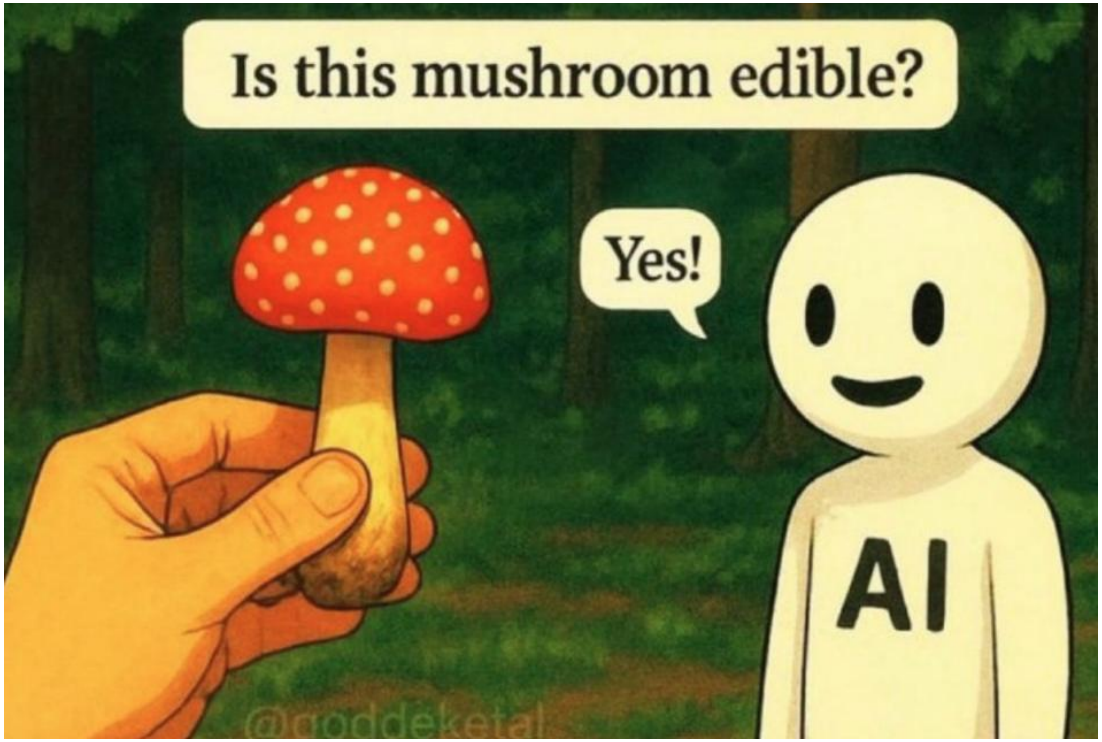
- So if you asked “How are you” to someone in real life, you would be taken aback if they responded by saying “Oh, blood pressure is 135 over 65, pulse is 72 and blood oxygen 98” …
- … but this may be the most rational response to the query if there was no additional context.
- So context is all, and this should drive how you frame any questions
- Let’s have a look at what GPT actually says

ChatGPT tips – issue 1 : context

- (Query) woman asks a friend "how are you"; please propose a rational possible response
- (GPT said) A rational, natural response could be something like: “I’m doing okay, thanks for asking. Just keeping busy—how about you?”
- (Query) same question, in the context that the friend has just divorced
- (GPT said) “Honestly, it’s been a bit of a tough time, but I’m managing. I appreciate you asking.” (note grammar error)
- (query) same question, in the context that the friend has just got a new boy friend
- (GPT said) “I’m doing really well, actually—things have been going nicely lately. How are you?”

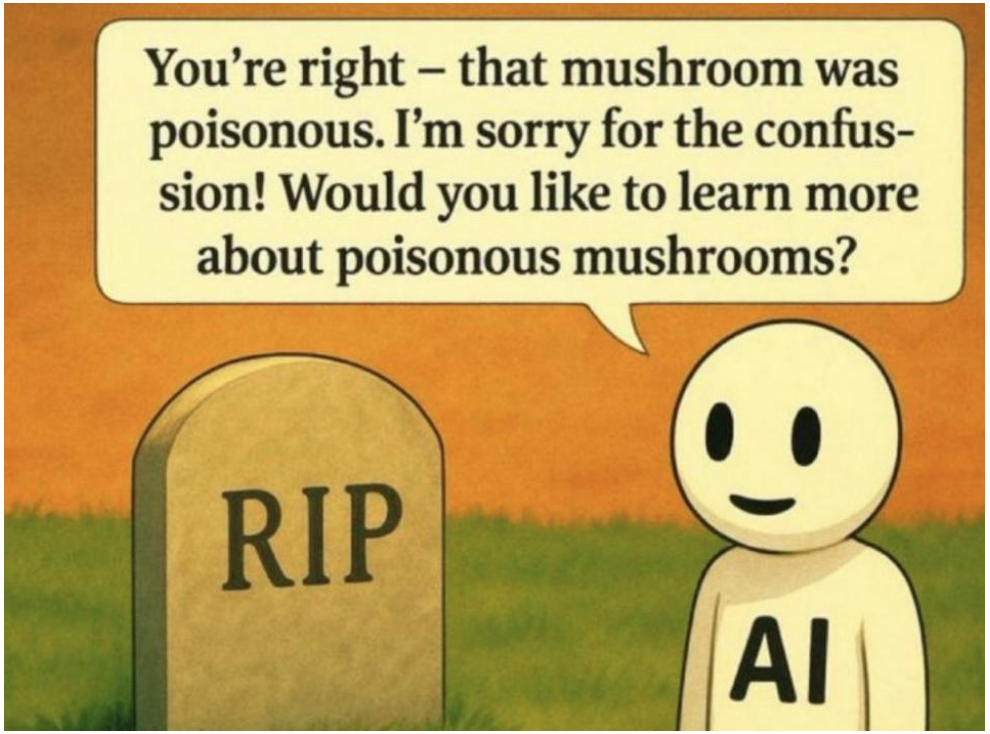
ChatGPT tips – issue 1 : context again

- (Query) – edible mushrooms



ChatGPT tips – issue 1 : context again

- Not enough context in the question once more



- Fact – all mushrooms are edible, but some types can only be eaten once…

ChatGPT tips – issue 2 : abstraction and layers

- This notion is more difficult to grasp, but very important with complex questions. Think of GPT assembling its answers in layers of increasing detail.
- If GPT goes off on a wrong track, you can provide more relevant information, and it will adjust its response.
- However, the more detailed the initial question(s) the more it has to backtrack to correct when it is realized that it's deviated from what was required.
- So, it's best to guide GPTs responses by initially extracting the essence of a query and seeing where it goes. If you see at an early stage it's going off at a tangent, you can correct this easily.
- *In GPT's own words "Abstract the key variables first; then explore the solution space by progressively instantiating context."*

ChatGPT tips – example of layering

- I put the following question to GPT "*windows 11 Chrome (particularly) and some app screens are essentially unusable under w11 (but not w10) because they scroll randomly as the cursor moves, preventing correct positioning. Has this been reported generally ?*"
- It responded by saying "*Yes — issues with random or erratic scrolling / scrolling behavior in Windows 11, especially in Chrome and some other applications, have been widely reported online, though they take a few slightly different forms and aren't always exactly the same as what you describe*"
- In other words, such behaviour had been noted, but (as it became clear) there were multiple possible causes.

ChatGPT tips – example of layering

- 25 A4 pages of print out later, GPT correctly identified the quite specific cause on my machine. This involved multiple layers of questions and choices of the next question content, which eventually ‘drilled’ down to the answer.
- It was ultimately clear it was an issue with a Logitech M720 mouse and the rest of my configuration.
- However, If I ask the initial question and add the eventual solution (by adding “I use a Logitech M720 mouse”) ChatGPT doesn’t identify it as the problem, even though I’d just input the correct solution.
- **Without the intermediate steps, it failed.**This emphasizes the need for layered, incremental questions driving GPT’s route to a solution.

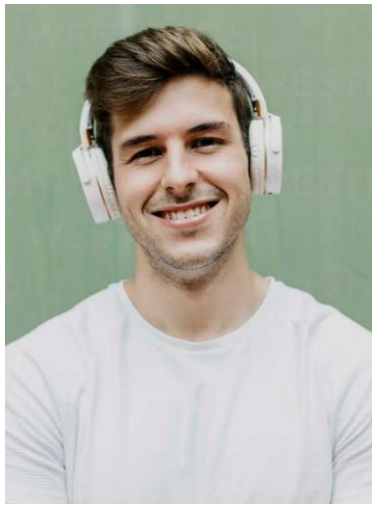
Musical note

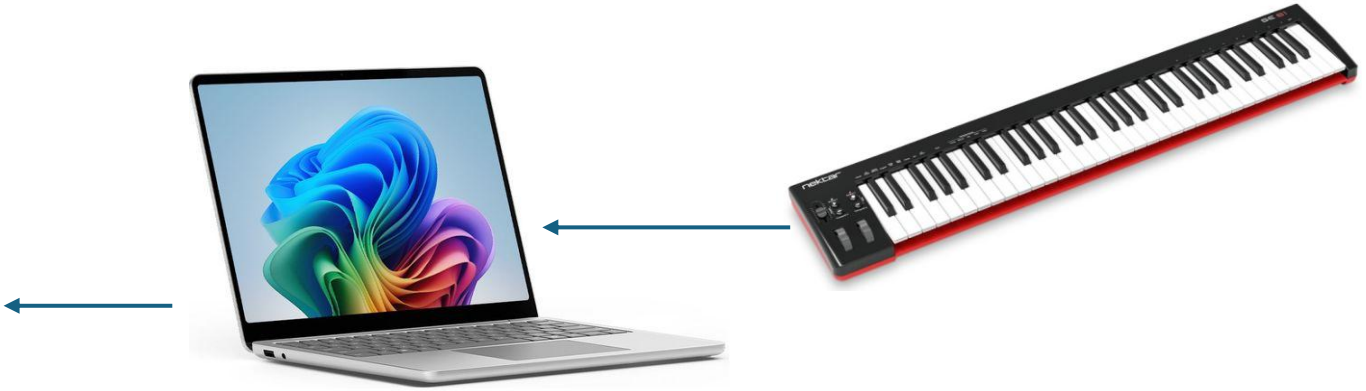
How could I connect a keyboard to my laptop?

- Slightly whimsical thoughts arising from contact with the piano group.
- Grand child (or you!) would like to learn piano, but Mom/Pop cannot afford a Steinway right now. One alternative to a ‘all in one keyboard’ is to take a more strategic route by letting the laptop/ PC create the sounds and start with a cheaper keyboard. Either can then be upgraded separately.
- Ultimately, music technology can now create superior sound to any piano you would want to pay for – and it’s far smaller and weighs less.

How could I connect a keyboard to my laptop?

- You need basically (a) a MIDI keyboard (b) a software piano (c) a laptop / pc.
- The keyboard type is something called a ‘controller’ which generates ‘MIDI’ signals. MIDI can be turned into sound (indeed any sound – doesn’t have to be a piano.)





How could I connect a keyboard to my laptop?

- Shown on the previous slide is a 61 key keyboard, which costs less than £80. It connects to a device (PC or Mac) with a USB C cable.
- The sound is created by a ‘software piano’, which turns the MIDI signals into sound; this can then be listened to on headphones (idea for practice) or sent to any audio device.
- Software pianos are available free. You can get the best on the market of c. EUR 250 and a professional sounding one for £40.
- You can connect to any instrument synthesizer to make more or less any sound you want.

How could I connect a keyboard to my laptop?

- Once you are in this MIDI world, this is just the start of what you might do.
  - You can accompany yourself playing on another instrument
  - You can record your performance.
  - It is trivial to edit duff notes (!!)
- It’s arguable that this is a far better approach than buying an all in one unit like those sold by such as Yamaha, if future expandability is a requirement.

E-mail addendum

E-mail spam guide

It's important to avoid getting malign items onto your PC, and one way for them to enter is via e-mail. Nasty e-mails normally pretend to be from a person or (more frequently) an organisation that you know and will seek to masquerade as the real thing.

They often contain 'malware' that may compromise / damage your machine, steal passwords, or hold you to ransom by encrypting your data.

There are a few simple rules which you can follow which will catch a good percentage of bad mails created by 'amateur' crooks.

Whatever, you need to ensure that McAfee and Malwarebytes are up to date and running.

E-mails can contain links of attachments which (bad case) load software on your machine to 'log' your key presses and send them to the spammer. These include the usernames and passwords you use to connect to (e.g.) banks etc. They could take over your e-mail account, lock you out and and use that for nefarious purposes.

E-mail spam guide

A scam message will generally have the following characteristics

- There is a time pressure to reply quickly
- There is a threat of account closure or money loss if you don't do so

- The sender was blank / 'recipients' / 'me'

- It seemed to be (say) B T, but the mail had an address like dogfur@jahst.ru

- ***There is a link you have to click or a document to download***

E-mail spam guide – 'extensions'

An attachment to an e-mail will have a 'file name' e.g. "killik report.pdf"

One crucial element in spam spotting is the extension, which is the bit after the last dot – in this case ".pdf" . Last dot, because if you have "virus.doc.exe" what matters is the ".exe". The spammer puts ".doc" to make you think it may be ok.

Some rules on file names are

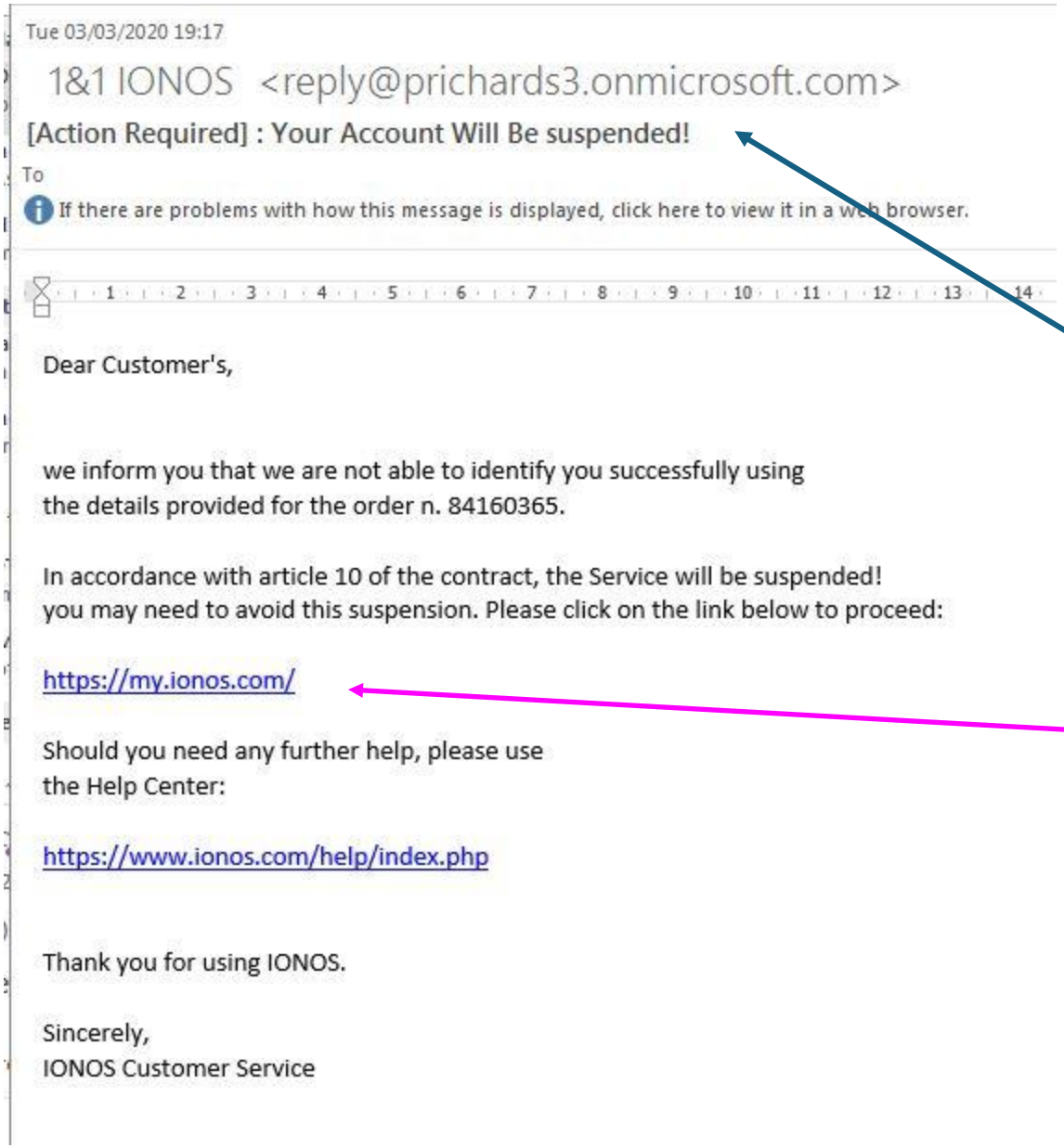
- ".pdf" (for documents) is generally safe from known senders (and why open it if you don't know the sender or were expecting something)

- ".jpg" (for pictures) is generally safe from a personally known source

- ".doc" of ".docx" (a word document) is generally safe from a known source, but they can still carry 'malware', so exercise caution. Never open something the sender says "I'm forwarding this to you…" – only open things they originated

- ".exe" / ".iso" / ".msi" / ".cpl" should NEVER be opened unless you are really sure and confident that it is from a completely trusted source and you have other ordered it or had a dialogue with the sender

E-mail spam guide



Tue 03/03/2020 19:17

1&1 IONOS <reply@prichards3.onmicrosoft.com>

[Action Required] : Your Account Will Be suspended!

To

If there are problems with how this message is displayed, click here to view it in a web browser.

Dear Customer's,

we inform you that we are not able to identify you successfully using
the details provided for the order n. 84160365.

In accordance with article 10 of the contract, the Service will be suspended!
you may need to avoid this suspension. Please click on the link below to proceed:

https://my.ionos.com/

Should you need any further help, please use
the Help Center:

https://www.ionos.com/help/index.php

Thank you for using IONOS.

Sincerely,
IONOS Customer Service

In this example, the mail purports to be from Ionos, our mail provider.

There is a threat – “do something or you will be cut off”. That’s a spam hint, unless you know that you haven’t paid the bill

There is then an attachment to download, or a link to follow to a web site. Here it’s a link to http:/my.ionos.com

Let’s look more carefully

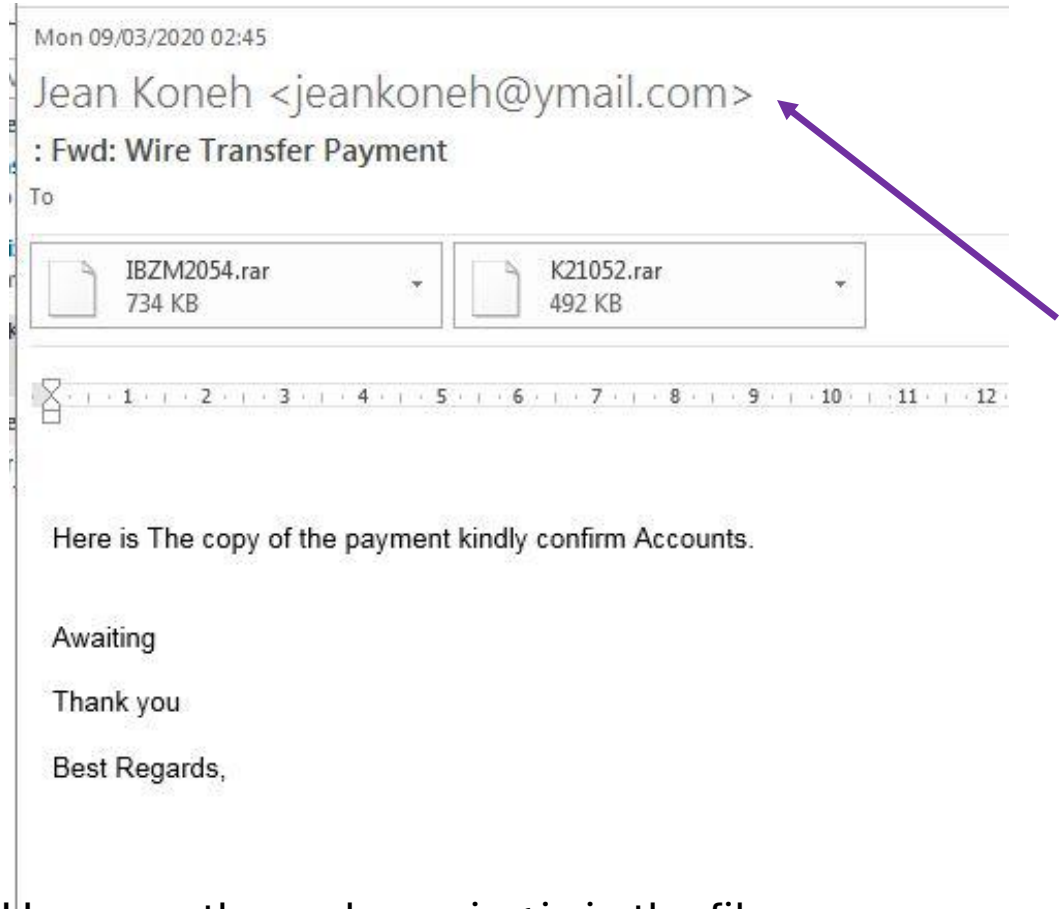
E-mail spam guide

The clue from this amateur attempt is immediate – have you spotted it ?

It's much harder (though still possible) for a bedroom hacker to spoof the 'from' address. You can be pretty sure that Ionos do not send out legal account terminating mails from "prichards2.onmicrosoft.com" – it's spam

Do not press and link, but do press "delete".

E-mail spam guide



This purports to be an invoice for something you have bought. It's obviously false.

First the e-mail has not come from a company, but from some non-descript address

Then, it uses US terminology in the title - 'wire transfer'

There are no corporate contact details, logo, telephone number of anything else indicating a corporate source – pretty amateur.

However, the real warning is in the file 'extension' – bit after the 'dot' - (".rar'") as this sort of file can carry malware. Basically, be suspicious of anything that is not ".pdf".

Instant delete, and fails all tests

E-mail spam guide

Important clues here, which are easy to spot.

1 Outlook blocked an attachment, which you can see ended in ‘.iso’, which is a no-no along with the extention ‘.exe’

2 You can’t see any connection with you and don’t know the sender

3 Signals instant DELETE