



Online Scams!

By The IT Doctors



George Saly

Why we get scammed

HEURISTIC

Heuristics are rules of thumb that help us make sense of the world and reach decisions with relative speed

SIMPLE: easy to understand, intuitive, automatic

SPEEDY: allows us to make quick decisions without much thought

EFFICIENT: requires less mental effort than other decision-making strategies.

BEST GUESSES: not always correct

may lead to COGNITIVE BIASES :

inaccurate or irrational decisions or judgments.

COGNITIVE BIAS

Cognitive bias is the tendency to act in an irrational way due to our limited ability to process information objectively.

A cognitive bias is an error in heuristic decision making.

When one internalizes a subjective perception as a reliable and objective truth.

Cognitive Biases Influenced by

- Emotions: “I’m under stress”
- Individual motivations: “I know better”
- Limits on the mind's ability to process information: “I’m busy”
- Social pressures “My brother has done this”
- **Age due to decreased cognitive flexibility: “\$%#\$#%^:”**

What about Scammers ?

Scammers target our cognitive biases

- **To make a fast decision.**
- **To not make a thoughtful decision.**

SCAMMER: Tactics

- **URGENCY:**
 - create a sense of urgency
 - pressure their victims into making quick decisions without thinking rationally
- **AUTHORITY:** may pose as an authority figure or use social proof (how our peers view us) to convince people that the scam is legitimate.
- **IMITATION:** use fake reviews or spoof phone numbers to appear more credible.

SCAMMER: Tactics (cont'd)

- **EMOTIONAL MANIPULATION:** may build a relationship with the victim through appearing to be likeable and establishing similarities.
- **OVERCOMING SKEPTICISM:** may use confidence and charm to overcome skepticism and objections.

Can I be SCAMMED?

!!YES!!

OUR TACTICS: When contacted

- Never give personal information
- Never contact 'them' using the contact information or the link 'they' supplied to you.
- Question **who** they are.
- Questions **why** they contacted you.

OUR TACTICS: Before clicking a link

- Read before you click
- Check the address
- Check the location of the link on the page
- Go to the actual web site.

OUR NEW YEAR'S RESOLUTION

1. I will **take my time**: there is no rush – “Let me double check!”
2. I will **verify**: Is this legitimate? - “Let me do some research about this”
3. I will use **my schedule** - “I will contact you later”
4. I will **not be embarrassed to** Use family, friends, lawyer, IT doctors, as a sounding board
5. I will **ignore the immediacy of the offer**: if it's legit, it will be available in an hour.

Dave Weiler

Examples

Phishing Email Example 1


- A threat to delete your iCloud storage
- Several clues that this is not legit:
 - Sender address is not Apple or iCloud
 - Link is not to Apple or iCloud
 - Feigned urgency – they want you to act immediately
 - Threat to delete all of your photos
 - “Your payment method has expired” – they are going to want you to enter your credit card information, which you should NEVER do using links from an email

The screenshot shows an email from 'Daveweiler, [ALRET]' with a subject line 'Your Photos and Videos will be deleted - Take Action!'. The sender address is 'newsletter@mrandmrsmith.com', which is annotated as 'Obviously not legit sender address'. A context menu is open over the sender address, showing options like 'Copy Address', 'Add to VIPs', 'Block Contact', 'New Email', 'Add to Contacts', and 'Search for "[ALRET]"'. The main body of the email contains a red warning box: 'Your payment method has expired: Update your payment information... If you don't have enough iCloud space, you can upgrade your storage plan'. This is annotated as 'NEVER update your payment information from an email link'. Below this is a blue box with the text: 'We failed to renew your iCloud storage !! Without icloud space, you may lose all your Stored data and files in iCloud service'. This is annotated as 'Threat'. The email then lists 'Order details:' including 'Subscription ID: 59838016', 'Product: iCloud Space', and 'Expiration Date: Wednesday 1 Nov 2023', which is annotated as 'Feigned urgency'. A blue button says 'Update my payment details', annotated as 'Link is not iCloud or Apple'. The email ends with 'Thank you for trusting us', 'Best Regards', and 'iCloud® Customer Service Team.', followed by a long, random-looking URL: 'http://lovegetty.com/aAcLZHSW.kM0t?Ari5Gv*LKkk8890F5*L*pRY37*pKJvV*L5*nyd*l0*RY0yt*LpzNC*LKKLY8'.

Phishing Email Example 2


- Similar to the previous example, they are warning that you have reached your storage limit, but in this case, they are cleverer, in that it looks more like a message Apple would send
- But there are still clues
 - In particular – the sender is not Apple or iCloud, and neither is the "Receive 50 GB" link
 - (hover over the sender name to see the sender address, or over "Receive 50 GB" to see what address this is linking to)

Threats



Cloud

You have reached you storage limit



Dear customer,

Your iCloud storage is full.

As part of our loyalty program, you can now receive an additional 50 GB for free, before files on your icloud drive are deleted.

Receive 50 GB

Link is not to iCloud or Apple

[http://platform.coinflux.com/DiAphDVO.OPQKWRI?aRi5GV\\$ikk8890f5\\$L\\$NIkkk\\$NjTWP\\$L5\\$n87\\$IX\\$Rs69p\\$C9GR\\$Lkklyw](http://platform.coinflux.com/DiAphDVO.OPQKWRI?aRi5GV$ikk8890f5$L$NIkkk$NjTWP$L5$n87IXRs69p$C9GR$Lkklyw)

Phishing Email Example 3

- This is another common one, because often we are expecting a shipment, or even if we are not, a message like this will make us wonder if someone sent us something
- There are the usual clues
- If you think there might be something coming from FedEx, go directly to fedex.com, don't use the link in the email
- Or if you think this might relate to an order from Amazon, go directly to Amazon.com

Daveweiler
Order ID#CA-6278585 has been **delayed.**
To: 6508582870586503@gmail.com
Reply to: Daveweiler

Spelling (points to 'delayed')

To: address is a numbered account at gmail, it should instead be my email address (points to '6508582870586503@gmail.com')

Sender address is not FedEx (points to 'newsletters@thestar.ca')

Grammar error (points to 'redelivery')

Thank you for choosing us! Support allows you to redelivery your package Today.

The package has arrived at the FedEx Transfer Center. Please confirm your Signature again .

This Scam is particularly effective if you were expecting a shipment. They want you to worry that if you don't act, the shipment won't get delivered.

It is asking you to update your signature, but they will probably also ask you to verify your credit card!

Package Details :

Order #:	#CA-6278585
Failed delivery :	18:00 AM
Status:	delivery Pending
Reason:	FedEx signature Needed.

Note: To ship your Order as soon as possible, simply click the button below to update your Signature and follow the progress of your Order.

Update my Signature (button)

Link is not FedEx (points to the URL below the button)

http://remote.liftengine.com/ddfdfd.fdfdqsAri5gV*LKKk8890f5*I*RYN1D*pKx8p*I5*n0mz*rLv9Q*67v0*IKkLzQ

Arrived at FedEx Location Center

Need Help?

If you need more help, please visit our [FAQs](#) section.

Phishing Email Example 4

- Subscription renewal notice is another common one, because our subscriptions do expire, and it is a good reason to ask for your credit card
- So if you think your McAfee subscription might be expiring, go to mcafee.com, or to the Settings in the McAfee app – don't use the link in the email!!
- (Note the threatening all-red background)

The screenshot shows an email header with the sender 'McAfee' and the subject 'URGENT: Your McAfee Subscription Expired...'. A red arrow points to the sender name with the text 'Sender appears to be McAfee, but when you click to examine, it is not'. Another red arrow points to the email address 'info_XMH@Marques251.onmicrosoft.com' in the context menu. The email body has a red background and contains the McAfee logo, a 'Prior To Renewal' warning, a 'Renew Your Subscription Now To Stay Protected.' button, and a list of steps: 'Step1: Click the button below to download the latest version of McAfee 2022.' and 'Step2: Run McAfee Antivirus to scan and remove all potential threats.' A discount of '62% 1 year extension discount' is offered, expiring on '23:59'. A link to 'Extend Subscription now' is provided, with a context menu showing the URL 'http://ironcitydist.com/oh7FryxT.JUEeT33BY?gAAAAABIF_YVik6a4Hn_GdBzg1dS7nyKYndE_w2riKlzlQ55CSw7qa1daH_rmPd5GfSz4-slop-0_SkuzM7rZbiCRMkvbyjt4HjvsNH9rpTa9-9jYp7nP50P4aAcsGzpsrbXW4LsyxVON06vm_qAR1wiL3lpQrpykw=='. A context menu is also visible over the link, listing options like 'Copy Address', 'Add to VIPs', 'Block Contact', 'New Email', 'Add to Contacts', and 'Search for "McAfee"'. On the right side, there are three annotations: 'They didn't use the correct McAfee logo:', 'No spelling or grammar errors, but there is feigned urgency, and an all-red background is used to emphasize the urgency.', and 'Link address is ironcitydist.com, not McAfee'.

McAfee™

Prior To Renewal :

Check Your subscription McAfee Device [Sat,30 Sep-2023](#) .
After the expiration date has passed, your device is prone to a lot various virus threats.

Your device may be unprotected, it can be exposed to viruses and other malware ...

Renew Your Subscription Now To Stay Protected.

→ what should i do?

- ☑ **Step1: Click the button below to download the latest version of McAfee 2022.**
- ☑ **Step2: Run McAfee Antivirus to scan and remove all potential threats.**

You are entitled to a discount:

62% 1 year extension discount

The offer expires on: **23:59**

Extend Subscription now

They didn't use the correct McAfee logo:

McAfee™

No spelling or grammar errors, but there is feigned urgency, and an all-red background is used to emphasize the urgency.

Link address is ironcitydist.com, not McAfee

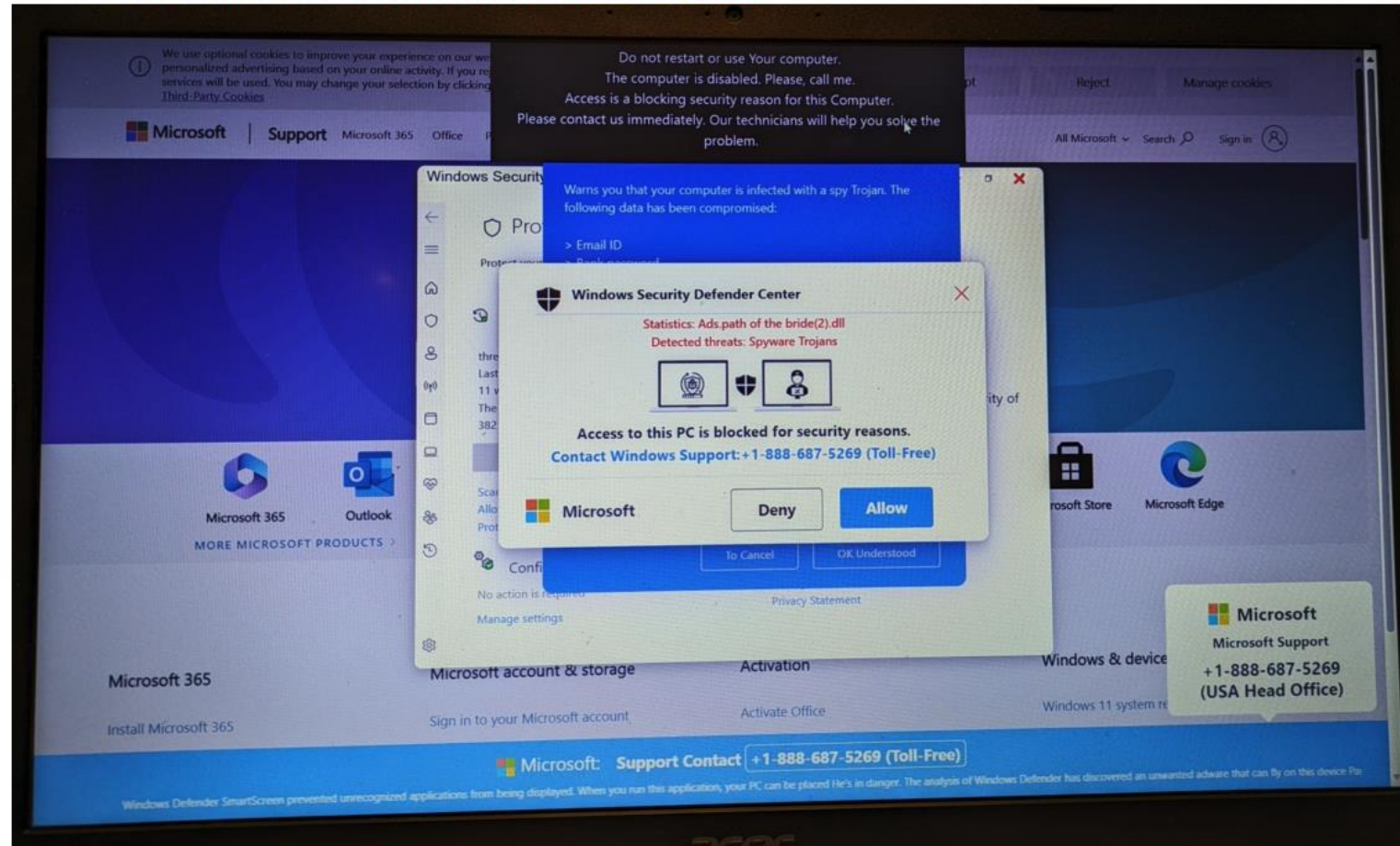
Ransomware 1

- More scary than phishing emails – you may find that suddenly you are unable to do anything on your computer, and there is a phone number to call for help
- This may overtly look like ransomware (“call us, or else”), or it might just look like a software problem
- Don’t call the number, and for sure **DON’T GIVE THEM MONEY!!**
- One example is shown at right – in this case, the browser is put into Full Screen mode, so that the tabs, task bar, close button, etc. are not visible

The website has forced the browser window into FULL SCREEN mode

- no Title Bar (on top), no Task Bar (on bottom)
- no Address (URL) bar
- no Close button

Trying to trick the user into believing their only option is to click Allow, because there is nowhere else to click



Try: Hit F11 (PC) or fn-F (MAC) on keyboard to exit FULL SCREEN mode

Ransomware 2

- This is something that happened recently – a member started up his computer, and after it appeared to start up normally, the screen went blank with just this message box. When he clicked OK, another message appeared giving him a number to call for help. When he called that number, they asked for money. When he restarted his computer, the message reappeared, and he still seemed to be completely locked out. Disconnecting from the Internet made no difference.
- He was of course afraid that someone had taken control of his computer, but in this case, fortunately that is not what happened. They were trying to scare him into sending money.
- He did the right thing: turned off his computer and called the IT Doctors for help!



Things You Can Do if it Seems That Someone Has Taken Control of your Computer

- Take a screenshot if you can. Or else take a screen photo with your smartphone. Even if the problem seems to then go away, a photo is something you can show us to help describe what happened
- Try F11 (PC) or fn-F (Mac) to exit Full Screen mode, and see if that then allows you to close the offending app or tab
- Try Ctrl-Alt-Del (PC) and select the Task Manager, and try to close offending app that way. On a Mac use Force Quit if available, or Option-Command-Esc.
- Shut off your computer and call the IT Doctors

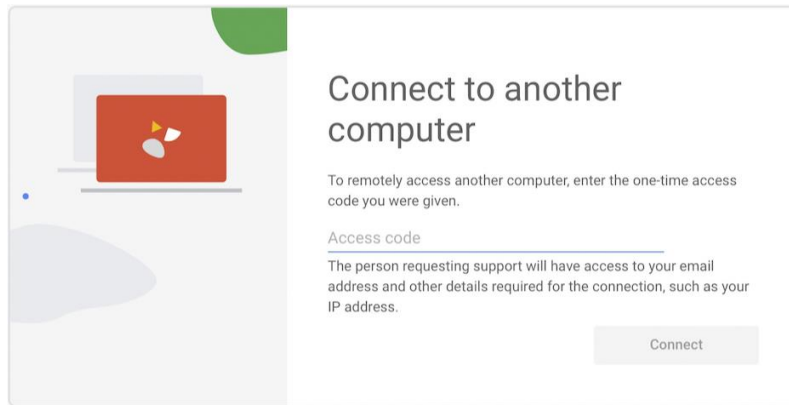


Virus Check after Ransomware threat

- Even if you are apparently successful in returning your computer back to normal, it is always a good idea to do a “Full” virus scan.
- The exact procedure varies depending on what anti-virus software you are using
- It is not likely that your computer is infected, but a Full scan can bring you peace of mind



Remote Desktop Software – be careful!



- Apps such as Chrome Remote Desktop, AnyDesk, and UltraViewer allow you to turn over control of your computer to someone at a remote location
- Be VERY selective about who you allow into your computer, don't be tricked into letting a stranger in just because he is offering to help



Pat Parno

Passwords

Nigerian Prince Died, and in his garage....



Password “Don’ts”

- Don’t repeat passwords!
 - Delete old website accounts
- Don’t answer Facebook questions like “Can you remember your teacher in grade 5?”. What’s your favorite color?
- Best not to use dictionary items or personal info
 - Rover1! Is not good
 - Pa\$\$word! Is pretty bad
 - Patrick123 is horrible



Password “Do’s”

- Bank passwords vs Aveda Hair Products passwords
- Can use the first letter of a sentence
 - 1 Really hate making up new passwords ! becomes 1Rhmunpw!
- can leave the vowels out of words
 - Canmore is a great place to live becomes Cnmrsgrtpltlv



Password Pass or Fail?

1. lhatepasswords
 2. j7Yk,eo(,eoc((Ee09322
 3. patISanITdoctor
 4. boxSCOREhatTERM
 5. iH8je&erjfJUyY7###4
 6. 1234567890
 7. Fred99canmore
- Problem is: good passwords are hard to remember!



Password Rules

- Length
- Upper and Lower Case
- Numbers
- special characters
- Why?



Size matters!

- $26 \times 26 \times 26 \times 26 \times 26 \times 26 \times 26 \times 26 =$ 0.2 trillion
- Add caps: $52 \times 52 \times 52 \times 52 \times 52 \times 52 \times 52 \times 52 =$ 53 trillion
- Add nums: $62 \times 62 \times 62 \times 62 \times 62 \times 62 \times 62 \times 62 =$ 218 trillion
- Add 10 sp char: $72 \times 72 \times 72 \times 72 \times 72 \times 72 \times 72 \times 72 =$ 722 trillion
- Now make it 12 chars = 2 with 22 zeroes after it
- Lesson: length is what matters



Password Recording

- Word file on your computer that is pw protected
 - Not “Notes” file on your phone!
- Writing them down in a booklet or paper is fine
 - Not on sticky notes attached to your monitor or desk
 - keep them updated!!!!
- Password Managers
 - Browsers: Edge, Chrome, Firefox all have ok ones, but then anyone using your computer can get in
 - Keychain if you have only Apple devices is fine. Google Password Manager is fine (and cross platform).



Password Managers

- Norton password manager. Free. Use across your devices
- 1password, Bitwarden, Lastpass, Roboform, Dashlane, NordPass, Keeper
 - from free to \$5 per month
- Note: if you use one of these, you must turn off your browser password filler. Otherwise they will both try to fill the password and bad things happen.
- demo



Summary

1. Slow down. Panic is what gets us scammed.
2. Check the address in the email. Check the link – official?
3. Don't click on a link and supply any personal info or passwords.
4. Go to the website yourself, not by clicking on a link.
5. Use Force Quit (Apple) or CTRL-Alt-Del (Windows) to stop a full screen takeover.
6. Use a virus scan regularly (Avast or Defender).
7. I am wary of Remote Desktops!
8. Record your passwords somehow, keep your list up to date.



Passkeys and 2FA

- Important! Who does not have a pin on their phone?
 - Your phone is going to be more important to id you soon; protect that phone
 - Using phone to make purchases is easy and safer than using your credit card
- Passkeys are coming!
 - Nothing to remember; phishing won't work on them
 - Can already use on MS, apple, google, amazon, eBay, Best Buy, FB etc
 - Not quite ready to use completely. Within 5 yr. though, should replace pw's
- 2FA – technically, any use of secondary checking on your login
 - Email, text, phone, other device, Authenticator.
 - Be careful with travelling! Banking story. Can shut it off or use email / other device. All banks have different methods.

