

Beware

Be Cyber aware

Josh Hollyfield



Phishing, vishing, smishing, spear phishing, whaling

No government agency is going to send an email as an initial point of contact.

Check the Reply address. The From address could say "person@greenhousedata.com"; however, the actual email address could be different, such as "persongreenhousedata@fraudulent.com."

It's hard to win something without actually participating in the drawing or game. Like winning the lottery without purchasing a ticket.

Some email clients, like Outlook, automatically block .exe, .bat, .vbs, .js file type attachments.

Big name companies and vendors check for spelling and grammar errors.

Reputable companies do NOT ask for personal information. If the message says it is from your bank, they already have your bank account number and PIN; they do not need you to send it to them.

Embedded URLs can be very misleading. The embedded link can be named anything the cyber criminal wants it to be, but if you hover your mouse over the link it will show you the actual URL destination.

Makes an unrealistic threat. Cyber criminals do this to scare people into giving them money.

Make sure it has the actual web address and not the web address followed by the parent (fraudulent) domain name.

Message

YOU JUST WON

IRS

Sent: Friday, December 5, 2014 2:33 PM

To: You

maliciouslink.exe (204.4 KB) (Preview)

Dear You,

Youve just one the lotery! In order to claim ur prize you need to fill out the attached form with you checking account info so that we can wire you the money.

After you fill out the attachment, click this link to claim your prize:

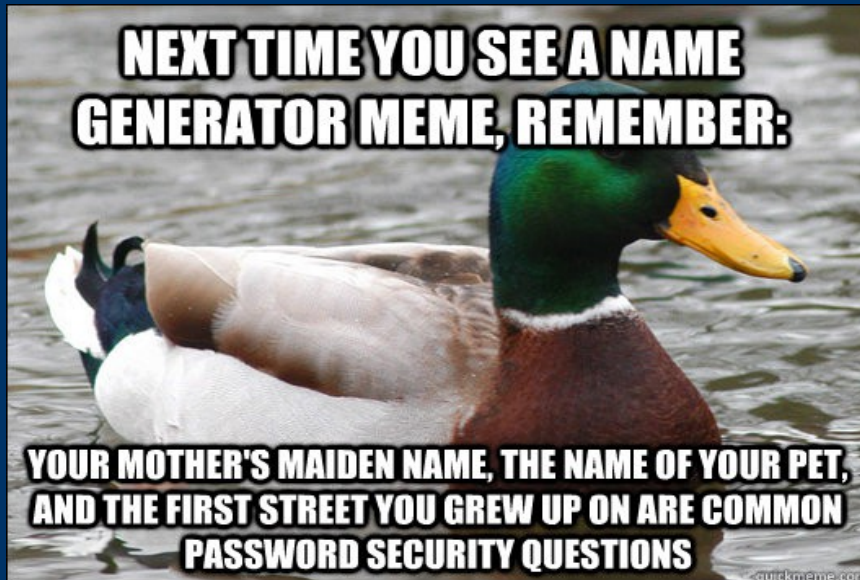
[www.lottery.com](#)

[www.lotto,maliciouslink.com](#)

If you don't claim your prize everything on earth will burn!

Social Engineering

- A manipulation technique that exploits human error to gain private information, access or valuables.
- Online or IRL



Passwords

- Keep your passwords strong and different
- Three words with numbers and special characters

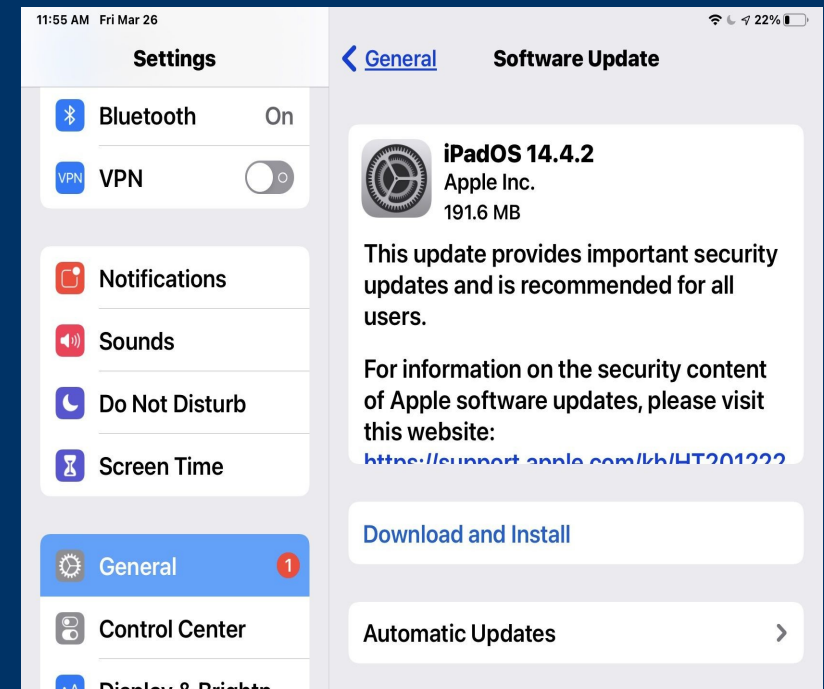
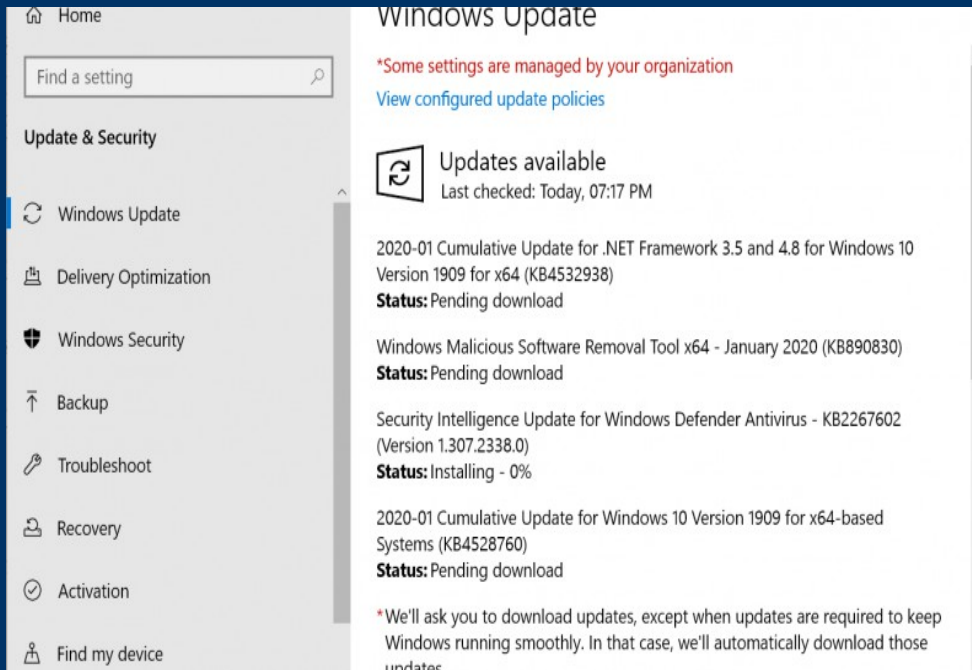
2FA

- Provides an added layer of security
- Something you know, have or are



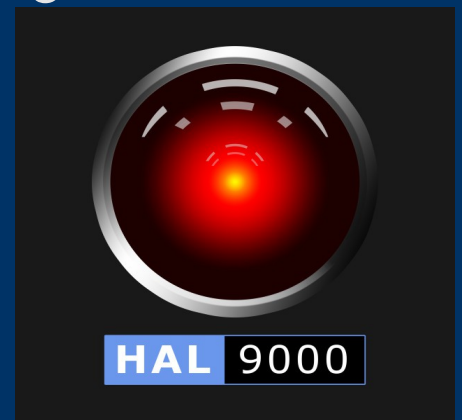
Updates!

- Please keep your devices updated.



Internet of Things

- The concept of connecting devices to each other and the internet and having the devices share information with each other.
- Devices can pose massive security risks.
- Buy from reputable manufacturers.
- Make sure you know what you're getting into when investing in these devices.



Phishing

Social Engineering Red Flags



FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they were **not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



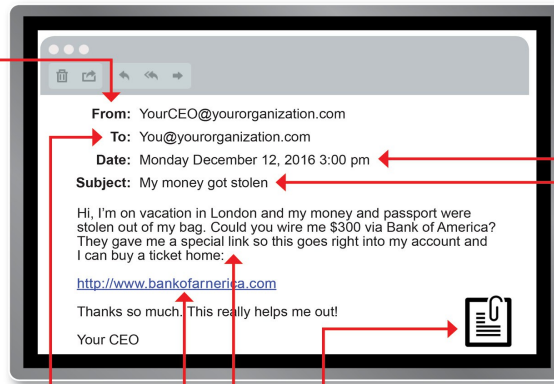
TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.



CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Malware

- Software that has been created to harm or exploit another piece of software or hardware
- Includes: Ransomware, viruses, worms, spyware and bots
- Good security practices: Not downloading files from unknown sources, having anti-malware software, not using your admin account for every day tasks



Backups

- Follow the 3-2-1 rule
3 copies, 2 different media, 1 copy off site



Thanks for listening
Thanks for understanding!
