




Cybersecurity Awareness

12/08/2022

Craig Hollis-Nicholson, KC3UOI

Cybersecurity areas of potential danger

- Viruses/worms/Trojan horses/malware/ransomware
- Attack vectors
 - Phishing/Social Engineering
 - Man-in-the-Middle
 - Weak password or security policies/user complacency
 - Physical security
 - Software bugs/vulnerabilities

A dark blue background filled with various cybersecurity icons. At the top center is a red circle containing a black silhouette of a person wearing a white mask. To the left of this is a blue folder icon with a white skull and crossbones. Below the folder is a red shield with a white checkmark. To the right of the masked figure is a white shield with a blue checkmark. Further right is a white spider icon. Below the spider is a red power button icon. In the center, there is a white Wi-Fi signal icon. To the right of the Wi-Fi icon is a red padlock icon. Below the padlock is a white router icon. In the bottom left, there is a red credit card icon. To its right is a white eye icon with a diagonal line through it. Below the eye icon is a red warning triangle with a white exclamation mark. In the bottom center, there is a laptop with a red padlock on its screen and a red progress bar below it. To the right of the laptop is a magnifying glass icon. In the bottom left corner, there is a grey envelope icon with a blue shield and a white spider on it. The text "Viruses/worms/Trojan horses/malware/ransomware" is written in a pink, serif font across the middle of the image. Below it, the text "How do cybersecurity attacks/events work?" is written in a smaller, pink, sans-serif font.

Viruses/worms/Trojan horses/malware/ransomware

How do cybersecurity attacks/events work?

Viruses

- A virus is any extra code that is hidden inside an otherwise benign file or program which causes some type of unexpected, harmful action, and which is triggered by opening the infected file/program.
- The virus is spread by passing the infected file around, often as an email attachment.
- There are thousands of known viruses “in the wild”, with many more discovered every week.
- They are mainly detected by antivirus (AV) software based upon known “fingerprints”, which requires AV software to be regularly updated with newest virus definitions database to maintain security.

Worms

- Worms are similar to viruses in that they are small pieces of code that discretely enter a machine to infect it. Unlike viruses, however, worms do not hide inside a file/program.
- Worms may produce multiple copies of themselves on the infected machine and upload copies to adjacent machines on the same network.
- Worms are detected by AV software using the same techniques for identifying viruses.

Trojan horse

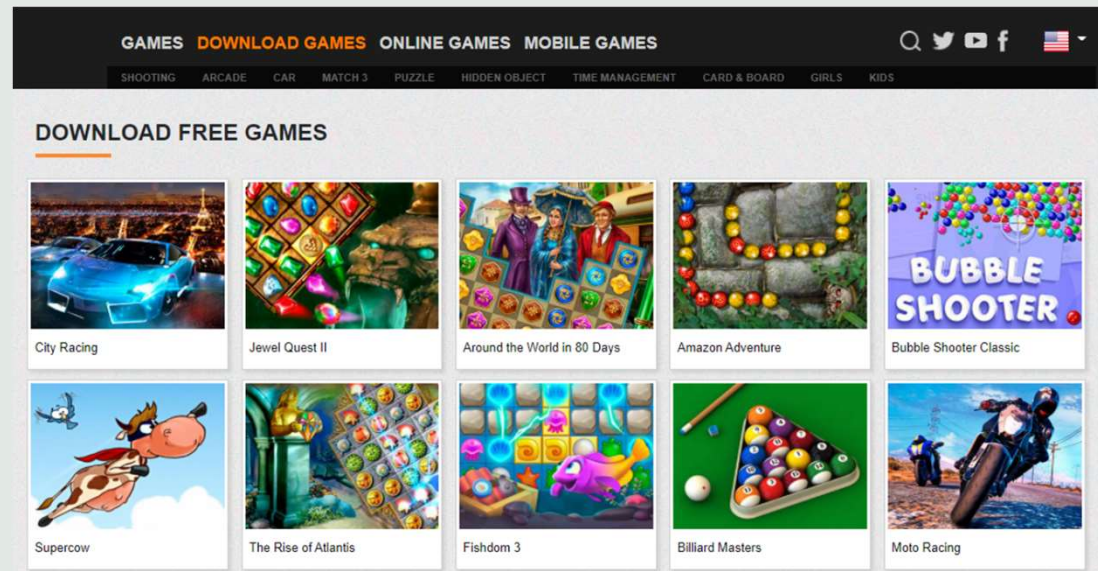
- “Don’t look a gift horse in the mouth” – Trojan horses are programs that appear innocent, but actually have a harmful purpose. Unlike a virus which turns a legitimate file/program into something harmful, Trojan horses are designed from the start to deceive the user into installing them.
- This is a closely related term to malware, but unlike malware (which generally does not cause permanent harm to data/your computer), Trojan horses actively corrupt their target machine.

Malware

- Simple definition: mal- meaning bad (from Latin), and -ware from software. Any software which produces an unexpected, negative effect for the device's user.
- Some subcategories:
 - Adware - software which relentlessly harasses the user with unexpected (often pop-up) advertisements.
 - Bloatware - software that comes preinstalled on a new computer but which the end user may have no use for and which needlessly occupies hard drive space.
 - Spyware - software that discreetly monitors the user's activity to collect personal information/credentials.
- Malware is technically not a virus, because it doesn't try to hide inside something else, and usually doesn't cause harm to the target machine or data. It may be a legitimate or useful program, but is also one that produces unwanted or unintended side effects.

Malware

- “Free” software sites are notorious for this, especially free PC games offered by no-name companies.

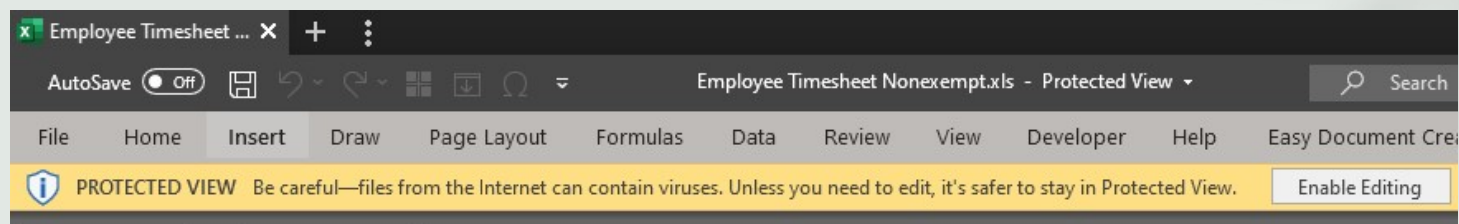


Ransomware

- Ransomware is a category of cyberattack where the attacker manages to obtain administrative access to a computer system. They then deploy a virus or worm to encrypt the data on that system, either the entire hard drive or at a minimum files stored on the system, using a password known only to the attacker.
- The attacker will then contact the victim to demand a ransom in exchange for the password to decrypt the victim's own computer and recover the victim's own data.

Protecting from harmful software

- Do not click on any link in an email where you are not absolutely 100% confident of the source of the message and know that it is legitimate. When in doubt, open a new browser tab and manually type in the URL to the website instead of clicking on any link provided.
- Do not download any attachment from any suspect email. If in doubt about an email's validity, contact the purported sender directly - phone call, creating a new email (do not reply directly to the sender of the suspicious message), meeting in person - and verify the email first.
- On personal devices, install and regularly update antivirus/anti-malware software.
- To mitigate the potential damage from ransomware, make regular backups of critical or irreplaceable data (3-2-1 backup rule), potentially including use of secure cloud storage.
- Enable OS features that are designed to protect your PC from cyberattacks





Attack Vectors

How do attackers gain access?

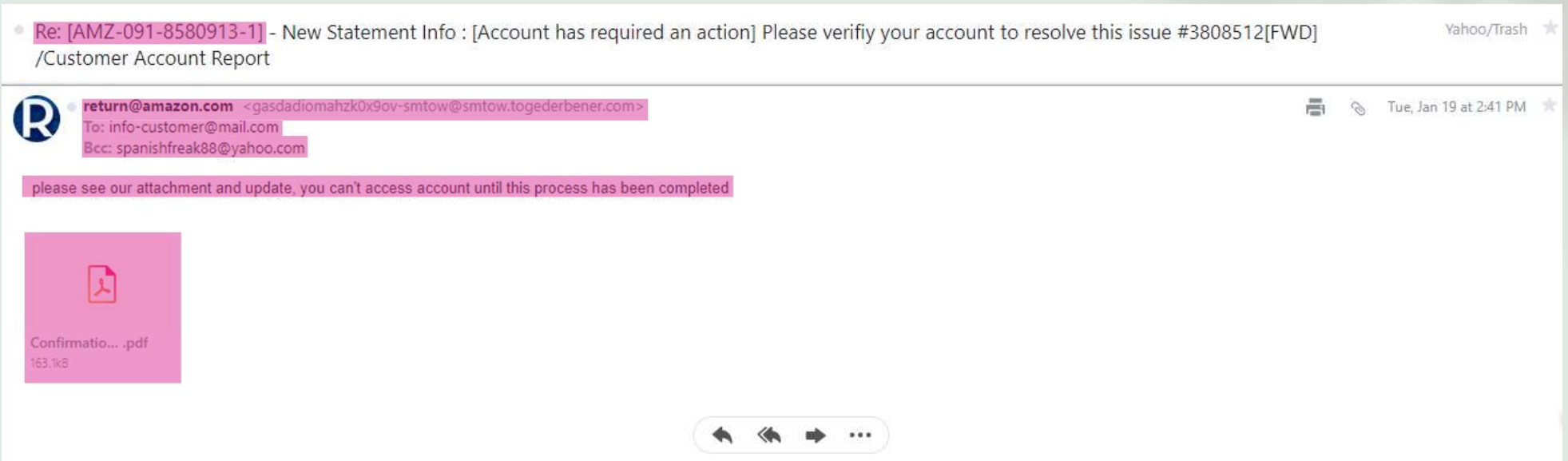
Phishing/social engineering

- Phishing is the act of coercing or tricking a user into providing their credentials or other personal information to an attacker. This gives the attacker access to whatever system/network the user has access to.
- Email is one of the most common sources of this type of exploit.
- Phishing attacks frequently utilize scare tactics to compel a user to take hasty action, making the user more likely to provide the desired information without thinking rationally about the request.
- Social engineering involves using psychological techniques to trick the caller into believing the attacker has a legitimate need for the user's credentials/personal information so that the user provides it willingly.

Phishing/social engineering

- Phishing is subdivided into several categories, depending on how it is accomplished:
 - Vishing - Voice (phone call) phishing
 - Smishing - SMS (text message) phishing
 - The term “phishing” itself is more recently used to refer specifically to attacks via email

Phishing email example



Legitimate email example



Yahoo/Inbox ★

 Tue, Jan 19 at 7:31 PM

Sent from my Samsung Galaxy Note 20 Ultra
Get [Outlook for Android](#)

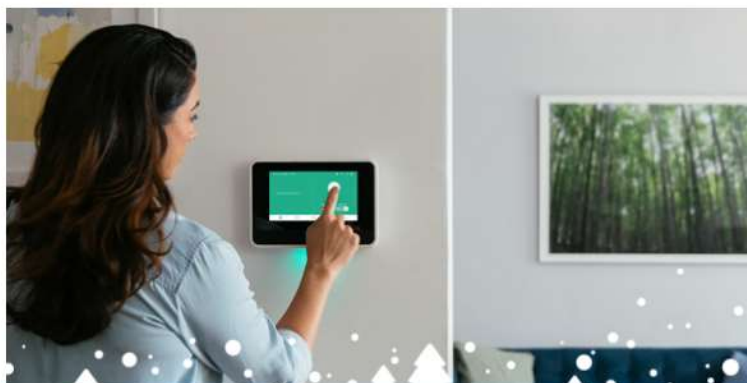
Sent: Monday, January 18, 2021 6:19:21 PM

Cc: jadeholl6466@aol.com <jadeholl6466@aol.com>

Subject: ``WelcomeTo VivintSmartHome``

A Safer Home Starts with Vivint.

1-866-481-1912



awaycleft.com/qs=r-acacaegfjhekaebfkibijaehgjiabababaceadbaccacbihackgjagkbhbach

Vivint Smart Home Security & AI

← → ↺ 🔒 https://www.vivint.com/home/vrb20?hf=true

Not syncing

.vivint Home Security Cameras Smart Home Services How To Buy Login 🔍

GET PEACE OF MIND TODAY

877.500.6716

Home Security Systems

Security Sensors

SMART HOME ALARM SYSTEMS

Smarter security, professionally installed

Find peace of mind with a Vivint smart home security system that's custom-built for your unique home.

CALL NOW TO CUSTOMIZE YOUR SYSTEM

877.500.6716

https://www.vivint.com/packages/home-security

Account Locked

From: no-reply@amazon.com (donotreply-styhkprilksybntmba@mdofficemail.com)

To: spanishfreak88@yahoo.com

Date: Sunday, December 4, 2022 at 02:07 PM EST



Hello spanishfreak88@yahoo.com,

We have temporarily placed your Amazon account on hold and canceled any pending orders or subscriptions because we detected unusual activity on it.

To restore your account, you can click the button below and follow on-screen instructions.

Once you have provided the required information, we will review it and respond within 24 hours.

You cannot access your account until this process is complete.

If you don't complete account recovery within 3 days, we will lock your Amazon account permanently.

We are sorry for any inconvenience this may have caused.
Thank you for your attention.

Sincerely,

Amazon.com

[Sign-in to Amazon](#)



© 2022 Amazon.com, Inc. or its affiliates. All rights reserved. Amazon, Amazon.com, the Amazon.com logo, and 1-Click are registered trademarks of Amazon.com, Inc. or its affiliates. Amazon.com, 410 Terry Avenue N., Seattle, WA 98109-5210.

Reference: 955842215

Please note that this message was sent to the following e-mail address: spanishfreak88@yahoo.com

- Attention! Important Information about your Social Security Number . Case ID:342657458



• **SOCIAL SECURITY INVESTIGATION 401538** <tjgjb181@gmail.com>

To: spanishfreak88

ATTENTION! spanishfreak88

Attention! Important Information about your Social Security
Number . Case ID:031098610
We have detected some wanted activities on your regular ssn.
Please take a look at the attached report for more details.

We have taken necessary measures to protect your account,

Thank you,

Social Security Administrator
United States of America

❗ Attachments cannot be downloaded. [Learn more](#)



case@investiga... .jpg

126.6kB

Database servers' updates

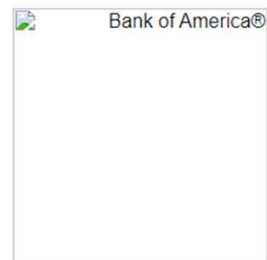
From: Bank Of America (info@franceslago.com)

To: spanishfreak88@yahoo.com

Date: Thursday, November 17, 2022 at 12:36 PM EST

For your security we disabled all images and links in this email. If you believe it is safe to use, mark this message as not spam.

[Show images](#)



New Account Security Update.

We've updated some features on your online profile.

We updated our database servers on Tuesday, November 17, 2022. To complete this update, you'll need to confirm your info and email address using the link below.

Go to, www.bankofamerica.com/date

- Sign on to your online account.
- One time code.
- Type your current debit info.

Thank you for banking with us.

Please don't reply to this automatically generated service email.

[Unsubscribe](#)

Billing update Without Tax

From: Norton Protesion Team (do_not_reply@intuit.com)

To: spanishfreak88@yahoo.com

Date: Friday, November 25, 2022 at 11:32 AM EST

For your security we disabled all images and links in this email. If you believe it is safe to use, mark this message as not spam.
[Show images](#)



Norton Protesion Team

Billingsupport@norton.com

Important Tax Information

Payment Processed to NORTON INC.

Date: 25th, November, 2022

Invoice Number: GT-581313

Dear Customer,

Here is your invoice. Ensure that you print or preserve a copy of your order after it has been delivered online for your records.

Please call our helpline. If you wish to review or cancel this order.

Call us :+1-(888)-701-3151

Order Summary :

Norton Protection Plan

Quantity : 1

Tenure : 3 Years

Total Amount : \$358.99

The transaction may not appear in your account for up to 48 hours. Your statement will list this transaction as "Norton Protection Plan."

Need help & Support :

Please contact us if you have a disagreement or if this payment was not made by you. Our customer support department may be reached at the given message:

Sincerely,

© 2022 NORTON INC. All Rights Reserved

+1-(888)-701-3151

Accept

★ **YOU HAVE WON AN *COSTCO* Reward**



.Congrats spanishfreak88 <118lkdslkdsodsd0e9eod09@lamatell.com>
To: spanishfreak88@yahoo.com



For your security we disabled all images and links in this email. If you believe it is safe to use, mark this message as not spam.

[Show images](#)

Congratulation Costumer!

You have Won a Costco Reward

Your Reward Code: #COSTC-CO924EF

Please Claim your reward before expiration.

GET STARTED*

* Please Note : All unclaimed rewards will expire due to the limited promotion

You may Unsubscribe [here](#)

Cranichols : Reminder 📦 delivery #2429105-UK560 Spam x



Pending Package (1) 📦 📦 TxySV0Bs82p3M...@qtqlnpanl.marchildren.in.net via w.economist.com
to 12.n]

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

UPS

**Your package delivery Notification
ID#34632900-371?**

TRACKING ID : 58412233520000

TRACK >>>

***We were unable to deliver your parcel as there was
no one present to sign for the delivery.***

***We are here to inform you that we need an address
confirmation to reconfirm the parcel shipping.***

CHECK HERE

for requesting to stop receive future email messages [click here](#).

The advertiser does not manage your subscription. If you prefer not to receive further
communication please unsubscribe [here](#)

★ 2022-11-25: Cranichols, You have won a 500£-----(J8DYRG)! Spam x



Tesco-Confirmation@ admin.DxT...@allison.renalcaculisurgery.info via w.economist.com
to 12.n]

8:21 AM (3 hours ago)



Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam



TESCO 500£

Congratulations Cranichols
You are a Winner

You have been **selected for using Tesco**, this email is Our
Official Notification Letter for your perusal.

choose from thousands of products!
Remember, you are one of the few selected, Registration is
only possible for the next 24 hours!

Limited supply! Be quick!

CLAIM YOUR 500£ GIFT CARD!

You may unsubscribe at any time [Unsubscribe](#)

• # No half-baked service for you. #



• **Invoice_Update_4866rj** <loganmarcueek@gmail.com>

To: spanishfreak88@yahoo.com



For your security we disabled links in this email. If you believe it is safe to use, mark this message as not spam.

<spanishfreak88>

Your e-receipt for product is here
check out your order-invoice.
Invoice Attached.

Your Receipt ID is PPL-azix5095638

If you have any questions or concerns, please don't hesitate to reach out to us at any time.

Thanks

This email was sent to spanishfreak88@yahoo.com at 11/25/2022 1:33:17 p.m..

🔴 Attachments cannot be downloaded. [Learn more](#)



p_a_y_p_a_l_g7... .pdf

59.6kB

• Re: PROJECT

Yahoo/Spam ☆



• **sarah mark** <msarah2020@outlook.com>



Thu, Nov 24 at 4:44 AM ☆

⚠ For your security we disabled links in this email. If you believe it is safe to use, mark this message as not spam.

Hello Confidant,

I am contacting you for a possible partnership to transfer US\$25, 000,000.00 to your country for investment under your assistance. Your sincere cooperation is anticipated and I will furnish you with the details, upon receipt of your response to this email address: jjj.joshua@yandex.com

My regards,

John Joshua.

★ You have won an \$500 Shell Gas Card

From: Shell Gas Station (4565sduisduid898e8es@iamatell.com)

To: spanishfreak88@yahoo.com

Date: Sunday, November 27, 2022 at 06:31 AM EST



ANSWER & WIN: A BRAND NEW!

\$500 Shell Gas Card



Congratulations! [spanishfreak88](#)

It will take you only a minute to receive this fantastic prize. \$500 Shell Gas Card

GET STARTED*

You have been chosen to participate in our Loyalty Program for FREE! It will take you only a minute to receive this fantastic prize

[You may Unsubscribe here](#)

Social Engineering

- Social Engineering is often utilized as a means to phish the victim for personal information.
- Actors who are well-practiced at social engineering are very smooth talkers and can be very effective at obtaining the information they are seeking.
- They may impersonate individuals in authority/superiors within a hierarchy of the victim's organization.

Social engineering video examples



Avoiding phishing/social engineering attacks

- Do not provide secure information (login name, password, etc.) to anyone whose identity you cannot personally verify. Most IT/administrative personnel shouldn't need to ask you for this information anyway, so always maintain a high index of suspicious regarding this type of request.
- When in doubt about the identity of a caller in this type of situation, hang up and place a direct call back to the agency or organization that the individual claims to represent in order to verify the need for this information.
- Defer any request for secure access to anything to IT/administrative personnel. This includes anyone presenting themselves as a vendor; if they are not previously vetted for access to secure locations, do not give them access without consulting IT/administration first.

Man in the Middle (MITM) Attack

- In this type of attack, the malicious actor either eavesdrops on a communication between the user and a legitimate organization/site or impersonates the legitimate organization/site.
- The attacker intercepts all communications sent to the legitimate site from the user, including login credentials.
- The attacker then sends back factitious responses to prevent the user from becoming suspicious.
- The effect of the attack is that the user believes they are interacting with the real site/organization, but in fact they are only interacting with the attacker. The attacker uses their data to access the real site in the user's place.
- UNSECURED public Wi-Fi is one of the most hazardous potential sources of a MITM attack.

MITM attack example



Defending against common MITM attacks

- Avoid connecting to unsecured public Wi-Fi connections whenever possible.
- If using public Wi-Fi is an unavoidable necessity, secure your connecting using end-to-end encryption; a VPN (Virtual Private Network) service accomplishes this for a modest fee.
- Only enter sensitive information (user names/passwords, credit card numbers, etc.) into websites that are protected by a secure (encrypted) connection (URL starts with https://).

Weak password policies/user complacency

A chain is only as strong as its weakest link.



Insecure passwords

- When a hacker does not possess the password to access a particular account, he/she may attempt to guess it. A “dictionary” attack begins by trying the most commonly used passwords first. The next step will be to try common English words (i.e., words found in a dictionary).
- Top 20 worst/least secure passwords of 2019*:
 - 123456
 - 123456789
 - qwerty
 - password
 - 1234567
 - 12345678
 - 12345
 - iloveyou
 - 111111
 - 123123
 - abc123
 - qwerty123
 - 1q2w3e4r
 - admin
 - qwertyuiop
 - 654321
 - 555555
 - lovely
 - 777777
 - welcome

*Source: <https://www.csoonline.com/article/3526408/the-25-worst-passwords-of-2019-and-8-tips-for-improving-password-security.html>

Insecure passwords

- We tend to choose passwords that are easy to remember. Easy to remember, however, also potentially means easy to crack/guess.
- Excellent (free) tool to verify the strength of any password:
<https://password.kaspersky.com/>
- Ideally, a secure password should contain a combination of capital and lowercase letters, numerals, and other special characters (\$, ., #, @, !, -, =).
- The strongest passwords tend to be at least 15 characters long.

15 CHARACTERS?? ARE YOU CRAZY?????

- An ideal compromise is to instead use a pass phrase. Phrases tend to be easier for us to remember than single “words”.
- Good example: 1L0V3G01NGT0TH3B3@CH (I love going to the beach). In this example, the number 0 was substituted for every letter o, 1 was substituted for i, 3 was substituted for every e, and the @ sign was used in place of the letter a. Even without using lowercase letters, it would be almost impossible for a hacker to guess this 20-character pass phrase. Using the password checker tool on the previous slide, it is estimated to take more than 10,000 **CENTURIES** to crack this one using the equivalent of a home PC, which is the tool most hackers would have.

Other guidelines to secure passwords

- Passwords (or pass phrases) should be changed regularly. Under CJIS requirements, this is a minimum of every 60 days.
- Never reuse old passwords/pass phrases, nor use the same credentials across multiple sites.
- Never use personally-identifiable information as the basis for a password/pass phrase (e.g., your name, birthdate, anniversary date, names of spouse/children, etc.). One tactic hackers use is to stalk potential targets on social media (or employ phishing) to harvest this type of information before starting an attack.
- Avoid common words (dictionary words) as passwords. **ESPECIALLY** avoid using any variation of the word "password" as a password.
- Secure password managers are a very convenient way to track multiple credentials, and are available as smart phone apps, web browser plugins, and standalone computer applications.
- Implement multi-factor authentication (MFA) wherever possible. This typically involves combining something you have (a token, your fingerprint, your phone, etc.) with something you know (a password) to authenticate yourself to a system.

Physical security



Physical security

- Physical security involves all of the engineering and physical measures intended to prevent unauthorized access to a system.
- Examples include PIN keypads, magnetic cards, physical keys and locks.
- Other examples would be locking a computer when it will be unattended by the user, restricting access by visitors to secure locations only, and positioning computer monitors so that they cannot be viewed by visitors.

Software bugs/vulnerabilities



Software bugs and vulnerabilities

- Probably one of the least-appreciated areas of cybersecurity is the vulnerabilities that exist in some applications as the result of bugs or known glitches in the programming code (or frankly just poorly-written software).
- As exploits are discovered, it is the responsibility of the software's developer to provide updated code that repairs (patches) these vulnerabilities to prevent future exploitation.
- Keeping software up-to-date and applying security patches as soon as they become available is a task for the end user (or IT) to mitigate these problems.
- "Zero-Day" exploits - refers to exploits of vulnerabilities that occur immediately after they are announced, before they can be patched.

Resources

- Cybersecurity awareness education and information:
 - <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content>
 - <https://www.csoonline.com/article/3340819/7-cheap-or-free-cybersecurity-training-resources.html>
 - <https://www.cisa.gov/stopthinkconnect>
- Password Managers:
 - <https://www.keepersecurity.com/personal.html>
 - <https://www.lastpass.com/premium-password-manager>
 - <https://www.dashlane.com/>
 - <https://www.logmeonce.com/>
 - <https://www.truekey.com/>

Resources

- VPN Clients

- <https://nordvpn.com/>
- <https://surfshark.com/>
- <https://www.expressvpn.com/>
- <https://www.tunnelbear.com/>

- Multi-Factor Authentication Solutions

- Google Authenticator - free app (available for [Android](#) and [iOS](#))
- Microsoft Authenticator - free app (available for [Android](#) and [iOS](#))
- [Yubikey](#) - hardware MFA (USB dongle)

Resources

- Antivirus/anti-malware software
 - <https://www.avast.com/>
 - <https://www.avg.com/>
 - <https://us.norton.com/>
 - <http://www.malwarebytes.com/>
 - <https://usa.kaspersky.com/home-security>

References/sources

- <https://store.hp.com/us/en/tech-takes/how-to-remove-malware>
- <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html>
- <https://antivirus.comodo.com/blog/computer-safety/computer-worm-definition/>
- <https://www.avast.com/c-hacker>