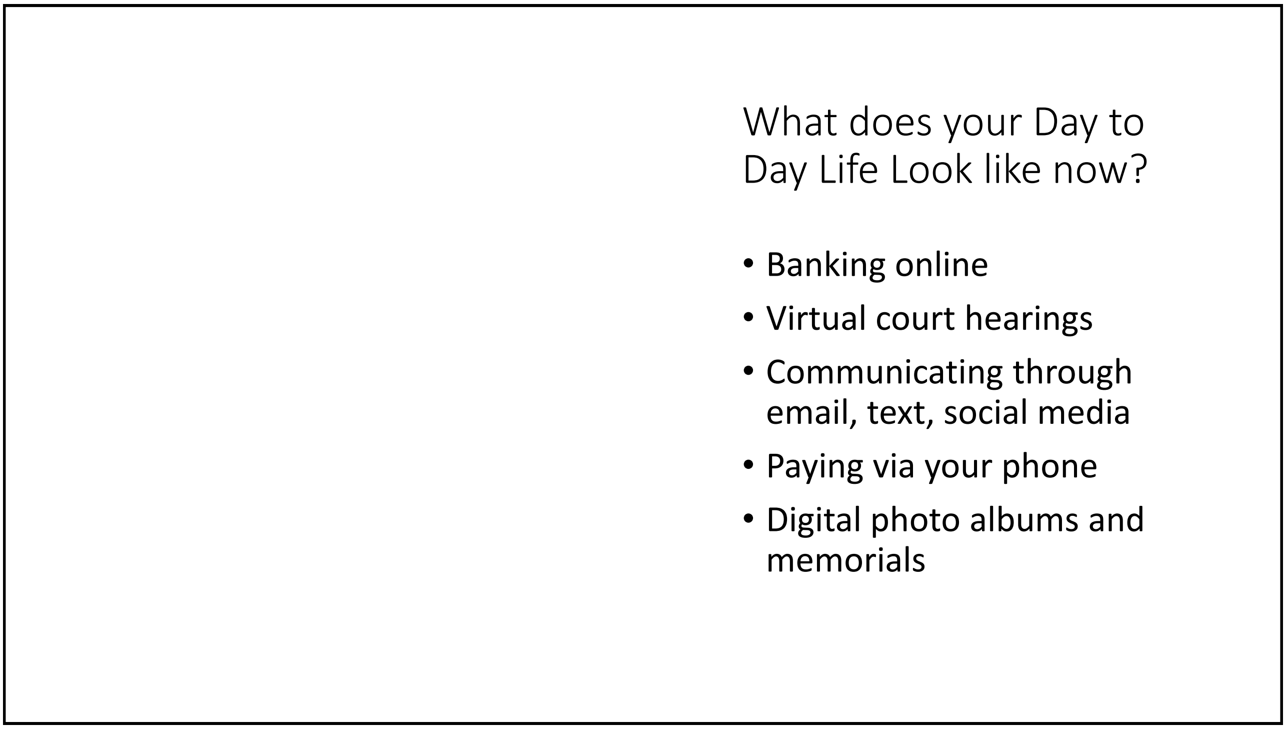
Spring Cleaning Series: **Cybersecurity in Your Court and Office**

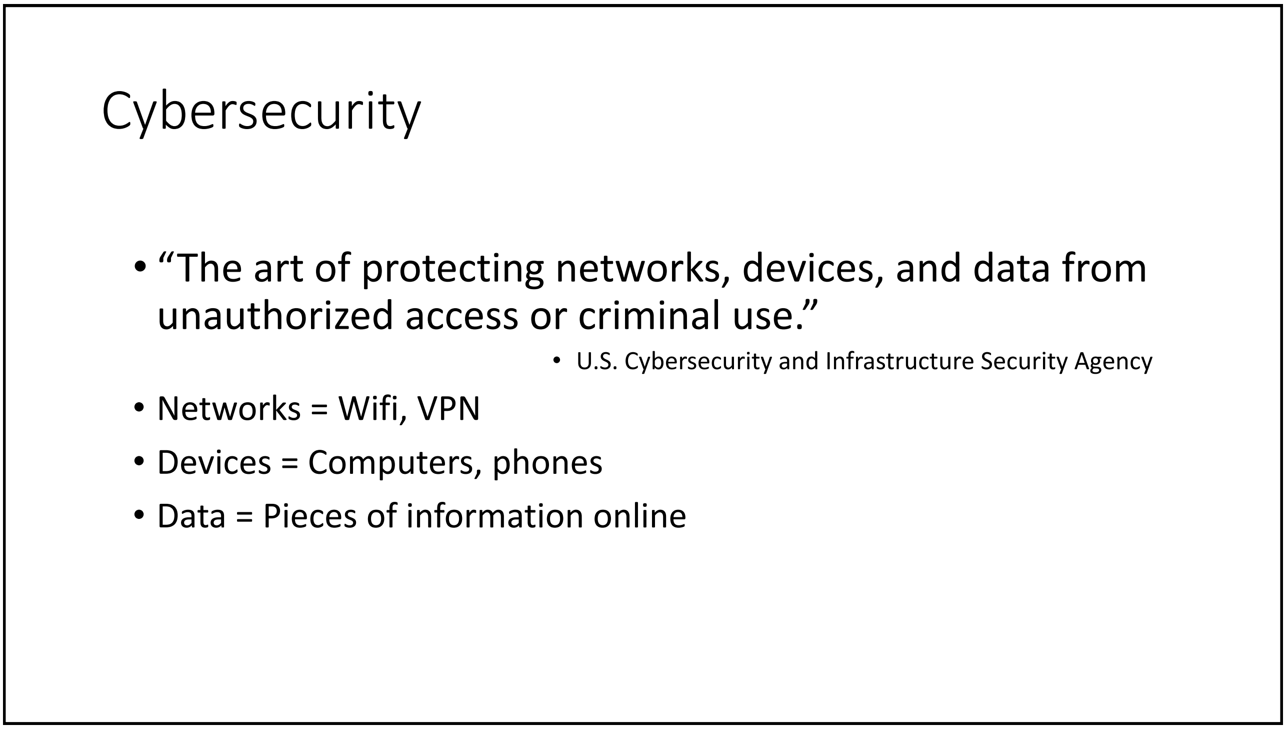
1



What does your Day to Day Life Look like now?

- Banking online
- Virtual court hearings
- Communicating through email, text, social media
- Paying via your phone
- Digital photo albums and memorials

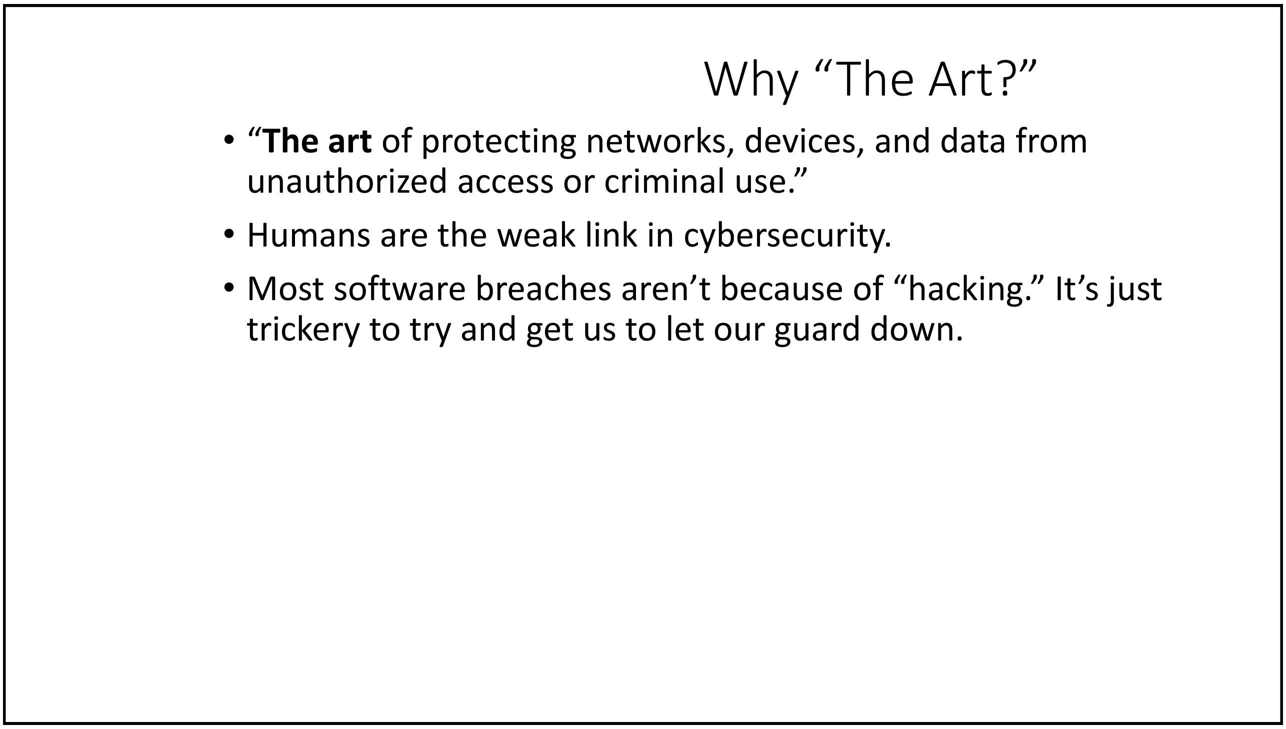
2



Cybersecurity

- "The art of protecting networks, devices, and data from unauthorized access or criminal use."
  - U.S. Cybersecurity and Infrastructure Security Agency
- Networks = Wifi, VPN
- Devices = Computers, phones
- Data = Pieces of information online

3



Why "The Art?"

- "**The art** of protecting networks, devices, and data from unauthorized access or criminal use."
- Humans are the weak link in cybersecurity.
- Most software breaches aren't because of "hacking." It's just trickery to try and get us to let our guard down.

4

Who is responsible for cybersecurity?

Here’s looking at you!

Every Single Person In Your Office!

5

Roadmap

How do scammers try to trick us?

What are they trying to do to our computers?

What are some best practices we can take to protect ourselves?

What policies and procedures should we review?

Where can we get more information?

6

Poll Question:

Have you or your office ever been the victims of a cybersecurity breach?

1. Yes, I have personally had information stolen.
2. Yes, our office has had a breach.
3. No, but I know of other people who have.
4. No, I haven’t heard of this.
5. I’m not really sure.

7

Recognize the Risks

How do scammers try to trick us?

8

Why Do people create Computer Viruses or Scams?

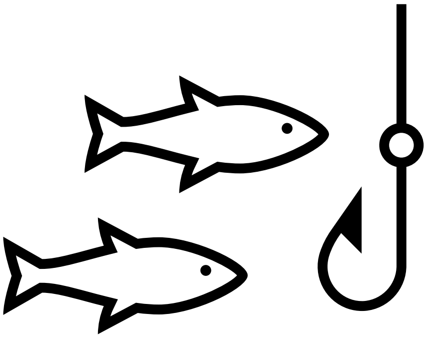
- 1. Financial gain
  - Think: Professional thieves want to harvest your data like credit card # for fraudulent purposes.
- 2. Prove themselves
  - Think: Hackers want to advertise how successful they are at creating computer viruses or countries want to show off their ability to control the web.
- 3. For the LULZ – To cause havoc
  - Think: A teenager wants to share pornographic images or cause trouble.

9

Types of Phishing = Scams to get personal info

- Phishing
- Cat Phishing
- Spear Phishing
- Whaling
- Vishing

10



What is Phishing?

Cybercrime where you pose as a trustworthy person/institution in order to obtain usernames, passwords, and sensitive information.

11

Phishing – How it works

- Send out a bulk email to a huge amount of email addresses.
  - Where do scammers get these email addresses?
- Oftentimes, Phishing isn't very sophisticated, but scammers are getting better and better.

12

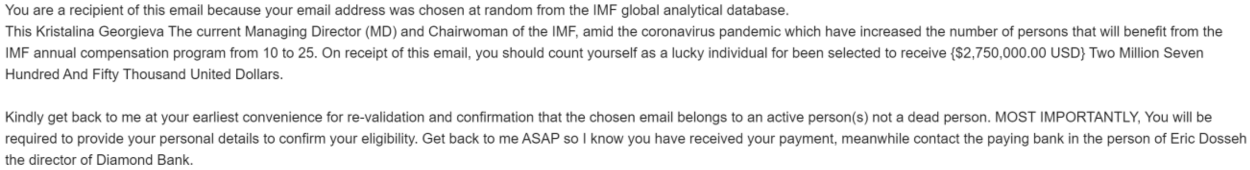
Phishing Example

- From: CEO@wellfargo.com
- Subject: Bank Password Expiring
- Dear User,
- The bank has implemented a new password rotation policy. Please login to www.wellfargo.com and update your credentials. You can also call 512-555-6872 and a representative can make the change for you.
- If you do not respond within 24 hours your bank account will be locked and funds unavailable.

13

Other examples

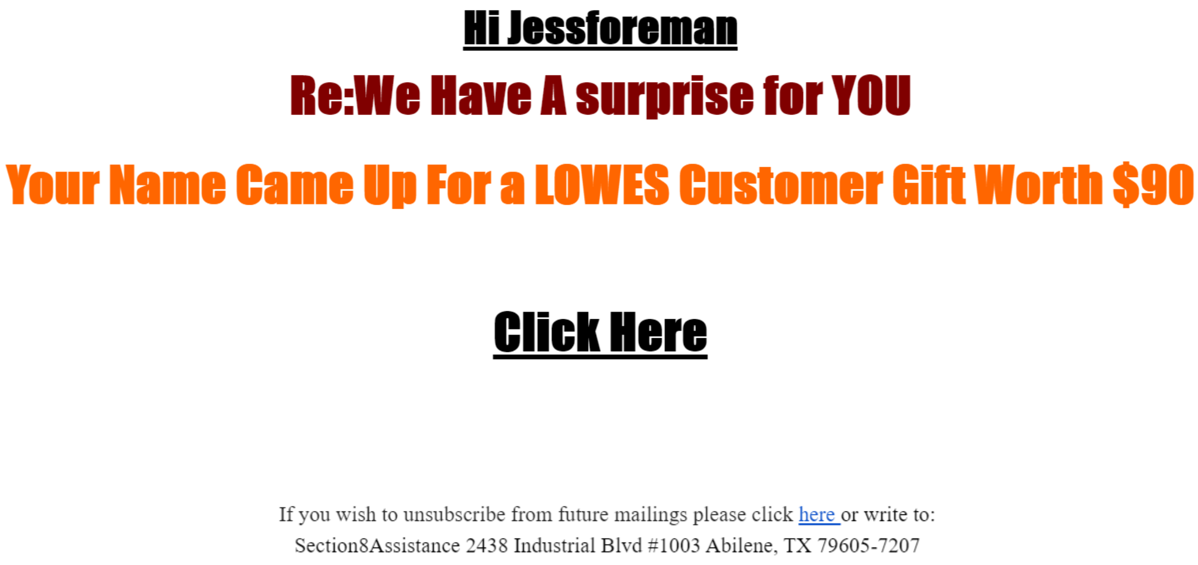
- You have been given a large sum of money from a long distant relative.
- Your bank account needs updating. Click here to update it with your SSN.



You are a recipient of this email because your email address was chosen at random from the IMF global analytical database.
This Kristalina Georgieva The current Managing Director (MD) and Chairwoman of the IMF, amid the coronavirus pandemic which have increased the number of persons that will benefit from the IMF annual compensation program from 10 to 25. On receipt of this email, you should count yourself as a lucky individual for been selected to receive {$2,750,000.00 USD} Two Million Seven Hundred And Fifty Thousand United Dollars.

Kindly get back to me at your earliest convenience for re-validation and confirmation that the chosen email belongs to an active person(s) not a dead person. MOST IMPORTANTLY, You will be required to provide your personal details to confirm your eligibility. Get back to me ASAP so I know you have received your payment, meanwhile contact the paying bank in the person of Eric Dosseh the director of Diamond Bank.

14



Hi Jessforeman

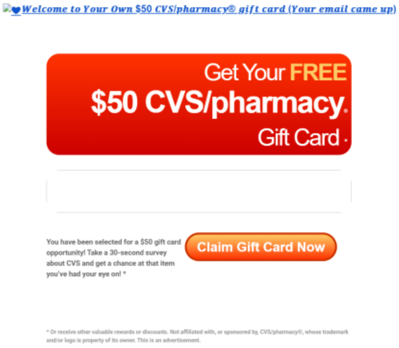
Re:We Have A surprise for YOU

Your Name Came Up For a LOWES Customer Gift Worth $90

Click Here

If you wish to unsubscribe from future mailings please click here or write to:
Section8Assistance 2438 Industrial Blvd #1003 Abilene, TX 79605-7207

15



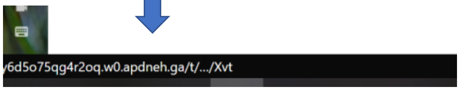
Welcome to Your Own $50 CVS/pharmacy® gift card (Your email came up)

Get Your FREE $50 CVS/pharmacy. Gift Card

You have been selected for a $50 gift card opportunity! Take a 30-second survey about CVS and get a chance at that item you've had your eye on! *

Claim Gift Card Now

* Or receive other valuable rewards or discounts. Not affiliated with, or sponsored by, CVS/pharmacy®, whose trademark and/or logo is property of its owner. This is an advertisement.



y6d5o75qg4r2oq.w0.apdneh.ga/t/.../Xvt

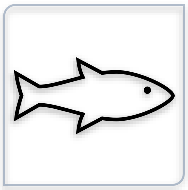
16

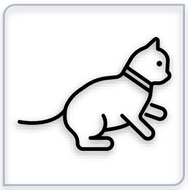
Phishing Best Practices – Don’t Get Hooked!

- A sense of urgency – “Act fast! Act now or else!”
- Too good to be true – “Free prize!”
- Hyperlinks – The spelling of the link versus the actual link
- Attachments – Not expecting an attachment? Don’t open it!
- Unusual sender
- No real organization is going to ask for confidential info over email
- When in doubt, call the company

17

Cat Phishing





- Faking an online persona
- The difference in regular phishing and catphishing?
  - Catphishing usually involves an online relationship of some kind. Maybe someone creates a fake profile with a headshot, etc. And eventually tries to swindle money or info.

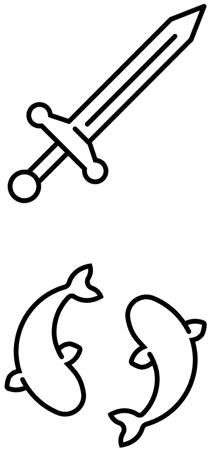
18

Cat Phishing – Don’t Get Hooked!

- Wary of people you don’t know well who are asking for money.

- Search by image to see if someone “borrowed” someone else’s photo
  - **“Google's** reverse **image search** is a breeze on a desktop computer. Go to images.**google**.com, click the camera icon, and either paste in the URL for an **image** you've seen online, upload an **image** from your hard drive, or drag an **image** from another window.”
    - From PCMAG.com

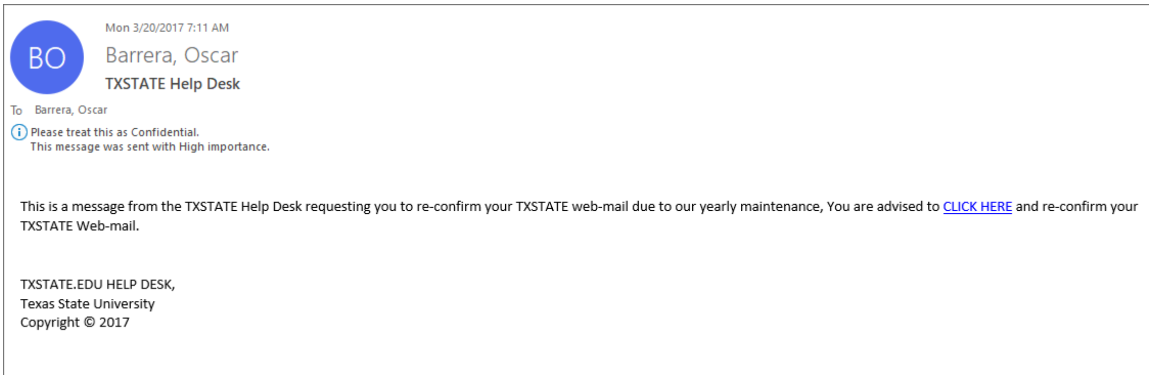
19



Spear Phishing

- A specific set of users or groups are targeted.
- The message is tailored to a specific group.
- This has a higher rate of success because it looks more real.

20



Mon 3/20/2017 7:11 AM

Barrera, Oscar

TXSTATE Help Desk

To Barrera, Oscar

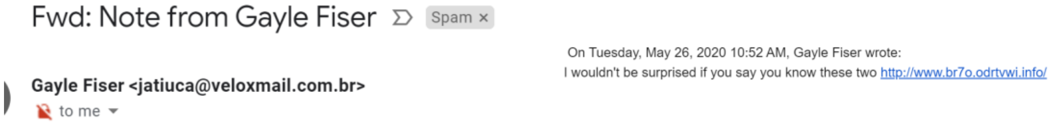
Please treat this as Confidential.
This message was sent with High importance.

This is a message from the TXSTATE Help Desk requesting you to re-confirm your TXSTATE web-mail due to our yearly maintenance, You are advised to CLICK HERE and re-confirm your TXSTATE Web-mail.

TXSTATE.EDU HELP DESK,
Texas State University
Copyright © 2017

-TxState
-Oscar is a real person

21



Fwd: Note from Gayle Fiser

Gayle Fiser <jatiuca@veloxmail.com.br>
to me

On Tuesday, May 26, 2020 10:52 AM, Gayle Fiser wrote:
I wouldn't be surprised if you say you know these two http://www.br7o.odrtvwi.info/

GAYLE FISER IS A RELATIVE OF OURS.
BUT WHY IS THIS EMAIL SUSPICIOUS?

22

Spear Phishing Example

- Example: Spear Phishing where a group of courts received fake emails that looked like they were from TJCTC accounts with an invoice they wanted you to download.

23

Poll Question

- Has anyone ever faked an email from your court or office in a spear phishing attempt?
- 1. Yes, we’ve had this happened.
- 2. No, this has never happened to us.

24

Spear Phishing – Don’t get Hooked

- Are you expecting this email? Is this the normal way that entity communicates with you?
- Are there any grammatical mistakes or does the language feel “funny?”
- When in doubt, follow up!

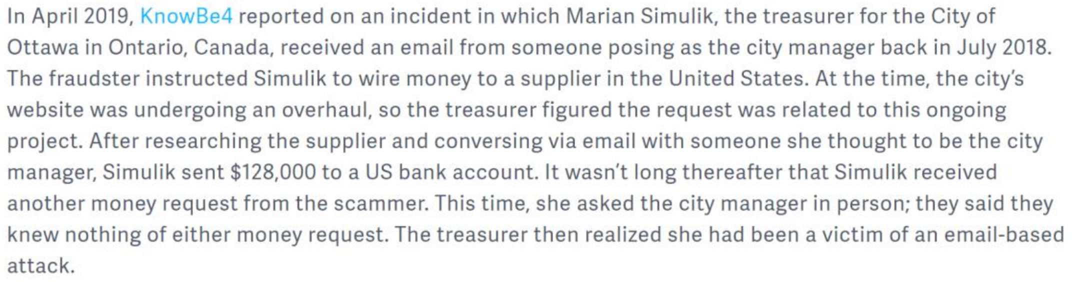
25

Whaling

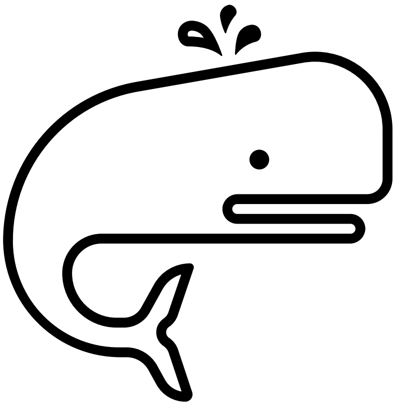
- An attack on a specific person. Usually an executive at an organization, but could also be a Judge or Constable or elected official.

26

Targeting county and city officials



In April 2019, KnowBe4 reported on an incident in which Marian Simulik, the treasurer for the City of Ottawa in Ontario, Canada, received an email from someone posing as the city manager back in July 2018. The fraudster instructed Simulik to wire money to a supplier in the United States. At the time, the city's website was undergoing an overhaul, so the treasurer figured the request was related to this ongoing project. After researching the supplier and conversing via email with someone she thought to be the city manager, Simulik sent $128,000 to a US bank account. It wasn't long thereafter that Simulik received another money request from the scammer. This time, she asked the city manager in person; they said they knew nothing of either money request. The treasurer then realized she had been a victim of an email-based attack.



Whaling – Don't Get Hooked

- Use your common sense.
- Be extra vigilant about clicking on links and downloading software.

Vishing

- Phishing done over the phone
- Automated recording
- Ask for credit card numbers, or something like this.
- “You owe the IRS money.”

29

Vishing – Don’t Get Hooked

- The IRS will never ask you for money.
- Is the person threatening? Or aggressive?
- Why are you receiving this call? Are you expecting it?
- If in doubt, hang up. Look up the company number and call to confirm.

30

What are Scammers trying to get you to do?

- More obvious trickery – Wire them money, directly give them your bank information or passwords
- Less obvious trickery – Get you to download MALWARE on your device.

31

Malware

Malicious
Soft**ware**

Be careful opening attachments.

Be careful downloading software.

32

Virus – Corrupts files

Trojans – Looks like real software, but opens up a security gap to let in other bad malware

Spyware – Software that spies on you in the background. For example, takes notes on your passwords and credit card numbers.

Ransomware – Software that locks down your files and threatens to erase them unless you pay a ransom

Adware – Not malicious, but allows for aggressive advertising.

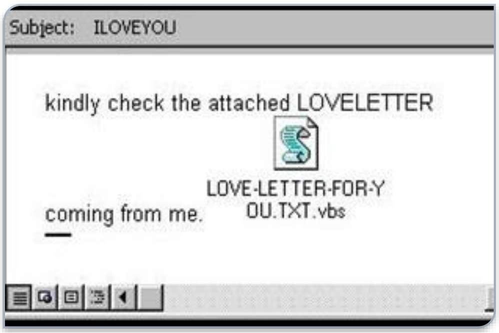
Think: pop-ups.

Botnets – Infects your computer and has it work with other computers under the control of an attacker.

33

Famous Virus

- I LOVE YOU message
- Subject: ILOVEYOU from secret admirer
- Kindly check the LOVELETTER coming from me
- ATTACHMENT: LOVELETTERforYOU.vbs



Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

LOVE-LETTER-FOR-YOU.TXT.vbs

Be careful opening attachments.

34

Trojan Example: Storm Worm

- Email with a subject line that said “230 dead as storm batters Europe.”
- When you clicked on the link, it would download software that would turn your computer into a “bot” or “zombie” and send a huge amount of spam mail.

⚠ Be careful opening attachments.

35

Spyware Example – Facebook Messenger

- On Facebook Messenger, you get a message from a friend that says something like: “Is that you?” or “XXX video.”
- You click on it, it downloads spyware on your computer, and spams your friend list with the same message.

⚠ Be careful opening attachments.

36

Poll Question:

- How many of you have seen the Facebook Messenger virus?
- 1. I accidentally clicked on it and it spammed my friend list.
- 2. I was sent it but did not click on it.
- 3. I’ve never seen this before on Facebook.
- 4. I don’t use Facebook messenger.

NEWS › COURTS

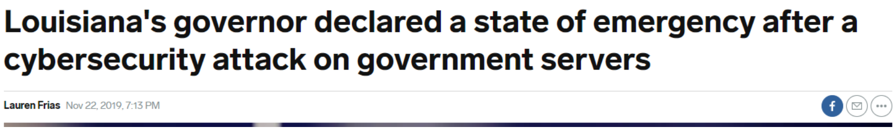
Texas courts hit by ransomware attack

State says there’s no indication ‘sensitive information, including person information, was compromised.’

System administrators discovered early Friday that hackers had taken over at least a portion of the statewide court network and demanded some form of ransom in return for restoring control. In a statement, the administration said the attack began “in the overnight hours” the same day it was discovered.

Ransomware

- 140 local governments including police stations, treasury departments, courts were hit with ransomware
- TxDOT and OCA



Louisiana's governor declared a state of emergency after a cybersecurity attack on government servers

Lauren Frias Nov 22, 2019, 7:13 PM

39

Unplug from the network
(Off wifi too)

Call IT department

40

ADWARE

Be careful downloading software.

- You want to download a video editor so you google “Video Editor.” One pops up and you download it. It asks for permission and you click “yes” without reading closely.
- While the video editor installs, it also installs a bunch of other software that you accidentally said yes to. It’s not necessarily viruses, but just software you don’t need that slows down your computer.

41

Best Practices For Good Cybersecurity

42

1. Be Savvy

43

1. Be Savvy

- Learn what scams are out there so you will be aware.
- Be careful when clicking links in emails from people you don’t know
- Be careful download software
- Even if it’s from someone you know, does it sound funny? Is it unexpected?

44

2. Keep Your Browsers UpToDate

45

What is a browser?

- The software you use to access the internet.
- Hackers are constantly trying to find vulnerabilities in browsers. Then companies find ways to fix those browsers.
- If you don’t keep them up to date, then viruses can sneak in.

46

Poll Question:

What browser do you use?

- Chrome (Multicolored ball)
- Firefox (Fox)
- Safari (Compass)
- Internet Explorer (e)
- Other browser
- I’m not sure

47

How Do I know If My Browser Is Up To date?

- See handout.
- *PROBLEM:* I have software I must use (like a case management system) that can’t run on the latest browser.
  - What can you do?

48

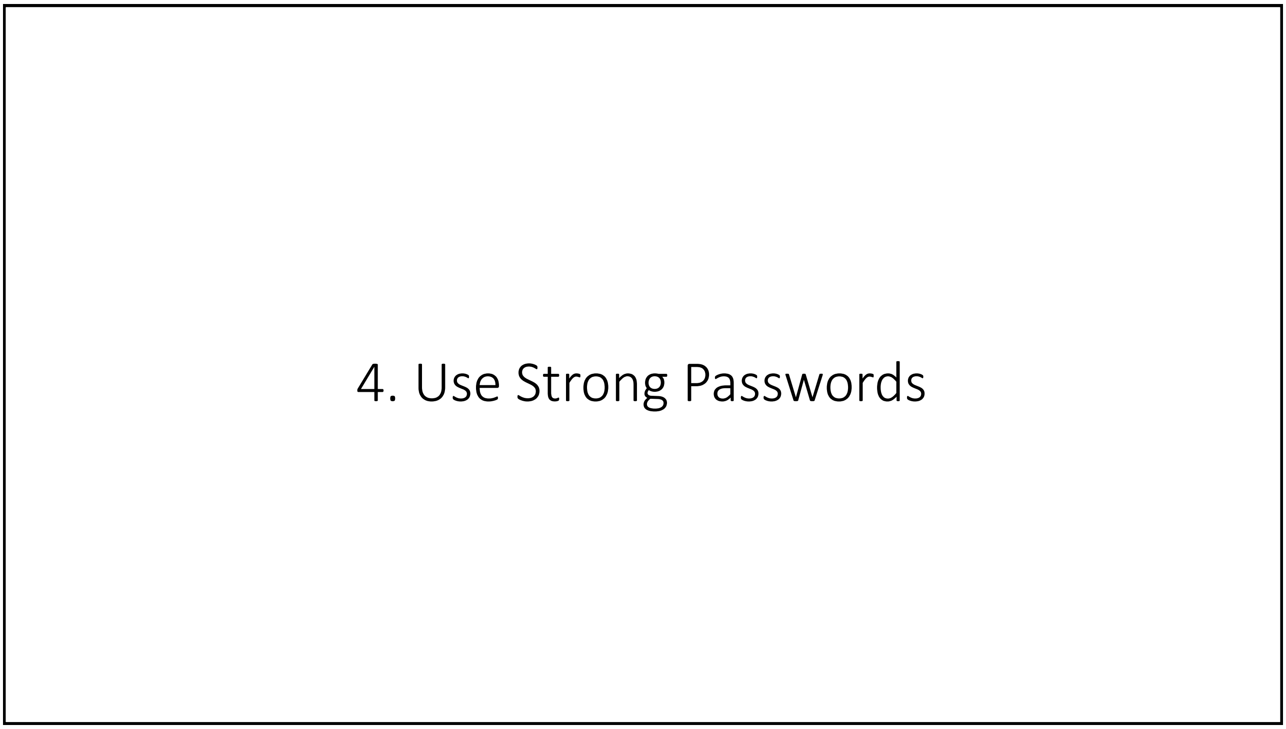
3. Run Good Antivirus software

49

3. Run Good Antivirus Software

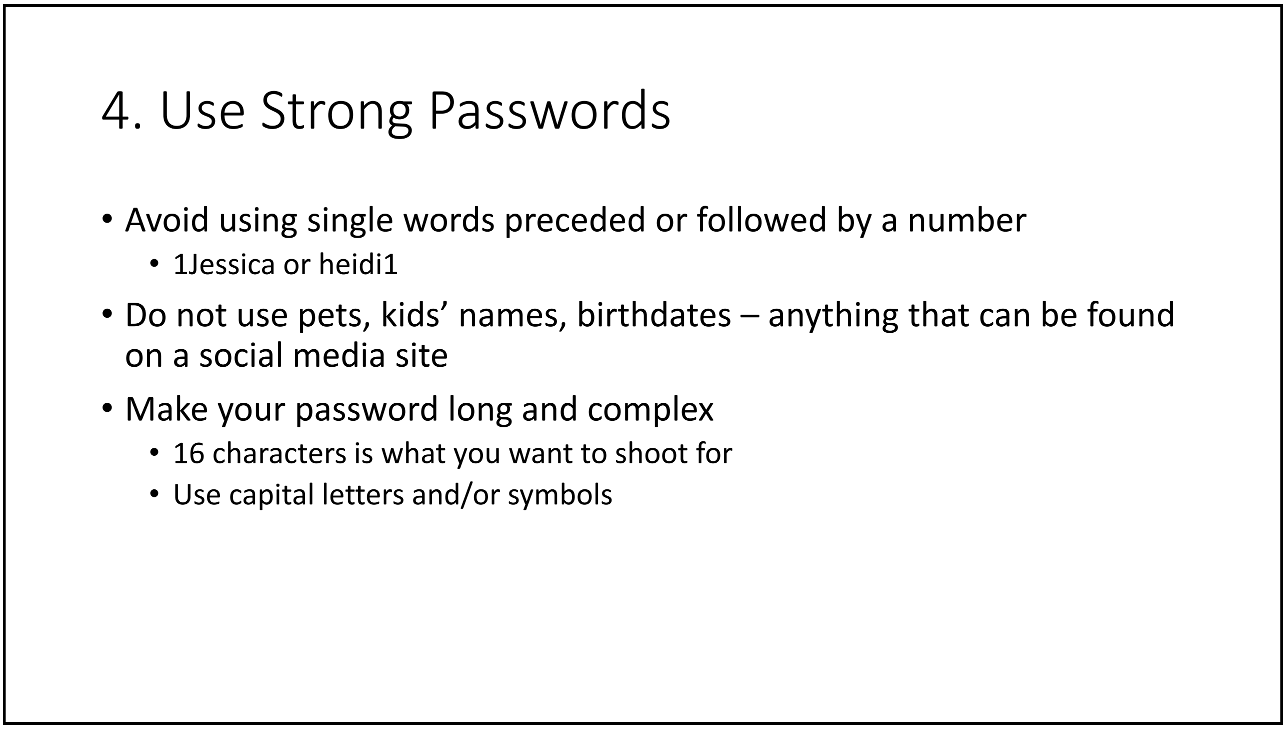
- What is antivirus software?
  - A computer program that prevents, detects, and removes malware.
- Popular ones: Norton, PCProtect, McAfee, Malwarebytes, many others
- What should you do?
  - Contact your IT department. What is your anti-virus software? Is it up to date?
  - Don’t just try to download something from the web. These generally cost money and you don’t want to download a shady free version.

50



4. Use Strong Passwords

51



4. Use Strong Passwords

- Avoid using single words preceded or followed by a number
  - 1Jessica or heidi1
- Do not use pets, kids’ names, birthdates – anything that can be found on a social media site
- Make your password long and complex
  - 16 characters is what you want to shoot for
  - Use capital letters and/or symbols

52

I can’t remember!!!!

Good! The safest password is one you don’t know.

53

Password Managers

Use a password manager. Password management tools, or password vaults, are a great way to organize your passwords. They store your passwords securely, and many provide a way to back-up your passwords and synchronize them across multiple systems. Though we do not recommend any one solution, here are some examples of free password managers*:

- LastPass: https://lastpass.com/
- KeePass: https://keepass.info/
- Keeper: https://keepersecurity.com/
- Password Safe: https://pwsafe.org/
- Dashlane: https://dashlane.com/

54

4. Use Strong Passwords

- Multi-Factor Authentication (MFA)
- Example of MFA:
  - After you log-in, you will receive a text confirming it’s you or a push notification.

55

5. Get to Know Your IT Department

56

5. Get to Know Your IT Department

- What are your county policies?
- Ask for a security audit.
  - And yes, if you do this, you will probably have to make some changes.
- Find out what software is approved for use

57

5. Get to know yOur County IT DeparTment

- Discuss how your data is backed up.
  - In case you do face an attack, make sure your information is recoverable.
- Discuss security software

58

What is your relationship with your county IT?

- 1. Good! They keep us up to date and we let them know about suspected security issues.
- 2. Good, but we don’t seem to work with them a lot on security issues.
- 3. OK, we don’t see them much/they are overworked/it’s not always a positive interaction.
- 4. I don’t even know who my IT contact is!

59

6. Know your Internal policies

60

Know Your Internal Policies

- Review your policies:
  - How often do you review your software?
  - How do you get new employees up to date?
  - What devices do you use to access work material? Your phone? Home computer?
  - Who has access to what data? Software? Passwords?

61

Do you use a shared email account?

62

Poll QuestioN:

Does your office have a shared email account?

1. Yes, we have more than 3 people with access.
2. Yes, we have less than 3 people with access.
3. No, we have a shared mailbox where multiple people can access, but each person uses an individual password.
4. No, we don’t share email accounts.

63

Shared Email Accounts

- What if an employee leaves?
- The more people who access the account, the more chances there are for accidental malware installations.
- What can you do?
  - Shared mailboxes – Office 365
  - Password Managers

64

7. Get in-Depth Training

65

State Mandated CyberSecurity Training

- https://www.county.org/Education-Training/State-Mandated-Cybersecurity-Course
- A new state law, HB 3834, effective June 14, 2019, requires all local government employees and elected officials who have access to a local government computer system or database to complete a cybersecurity training program certified by the Texas Department of Information Resources (DIR) at least annually.

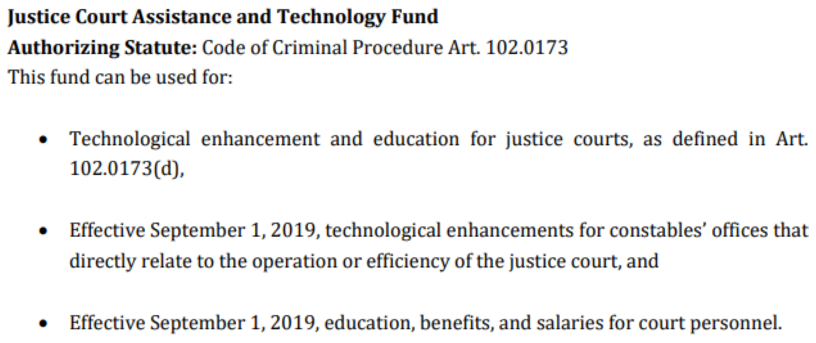
66

Other Training Opportunities

- *See handout.*

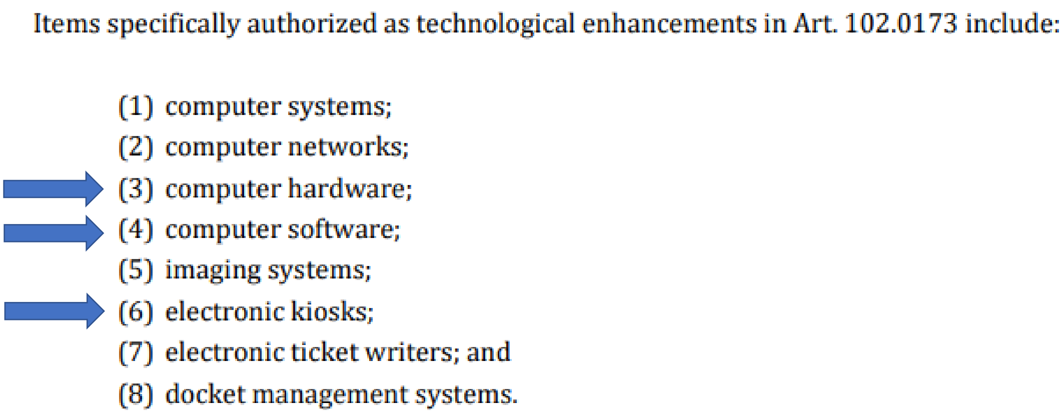
Buy, Buy, Buy: Where to get the money?

- TJCTC Fines, Fees, and Costs Deskbook



Justice Court Assistance and Technology Fund
Authorizing Statute: Code of Criminal Procedure Art. 102.0173
This fund can be used for:

- Technological enhancement and education for justice courts, as defined in Art. 102.0173(d),
- Effective September 1, 2019, technological enhancements for constables' offices that directly relate to the operation or efficiency of the justice court, and
- Effective September 1, 2019, education, benefits, and salaries for court personnel.



Items specifically authorized as technological enhancements in Art. 102.0173 include:

(1) computer systems;
(2) computer networks;
(3) computer hardware;
(4) computer software;
(5) imaging systems;
(6) electronic kiosks;
(7) electronic ticket writers; and
(8) docket management systems.

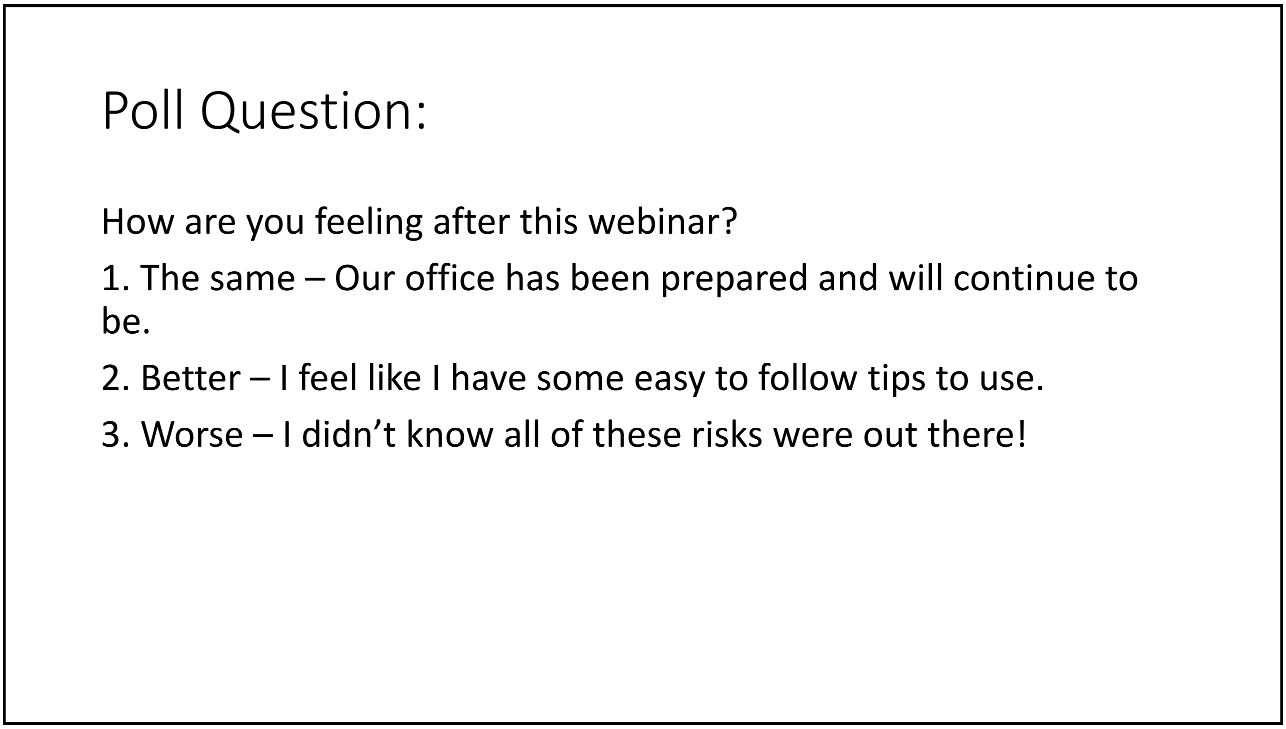
69

To conclude

Cybersecurity is everyone's job.

But these simple steps can protect you. It's not rocket science!

70



Poll Question:

How are you feeling after this webinar?

1. The same – Our office has been prepared and will continue to be.

2. Better – I feel like I have some easy to follow tips to use.

3. Worse – I didn’t know all of these risks were out there!

71