

Keep Calm

and

“Trust no one.”



# Why The Topic of Cybersecurity?

Around the time ALL approached me, my parents had their identities stolen!

- Despite doing everything “right”, it kept happening.
- So let’s discuss why.

Then that got me thinking about all everyone deals with online these days:

- Malware & Viruses.
- Scams.
- Social media and “low tech” crimes.
- Disinformation.
- Cyber-warfare.
- Deepfakes...

# Let's look at Malware and Viruses!

Malware is just malicious software...of various types.

## Viruses:

- Replicates themselves through the device.
- Originally destructive, now mostly for moneymaking.
  - Often used as "Ransomware."
    - For more Information, I've included an embedded video after the Conclusion slide.)

Never pick up and plug in a random USB drive.

- Be wary of ones at events even!
- Sort of funny, but Nine Inch Nails, the band, used to use USB drives left in bathrooms as part of the promotion for their Year Zero Album.

# Let's look at Malware and Viruses!



## Worms:

- Self replicate, spread, and burrow into the system.
- First one was in 1988!!
  - The Morris Worm was made to see if the concept worked...and nearly destroyed the early internet before most of the public had access.

## Trojans:

- A type of worm, disguised as a different file.
- Napster, back in the early 2000s, was the bane of many an IT administrator at my high school due to trojans disguised as music.



## How do we Defend Ourselves?

Patch that system! Just say Yes to the Windows Update feature – annoying as it can be.

Use an anti-virus/internet security suite.

- Contains a firewall, anti-virus software, etc.
- Personally I use Webroot's Spysweeper, but know folks who prefer things like Norton or Kaspersky.

# How about Scams?

- One of the top things to beware of online these days.
- Let's start with Phishing:
  - These pretend to be legitimate, but aren't. This image helps look for the signs we're going to discuss together!

The image shows a screenshot of an email with several red boxes and blue callout numbers pointing to specific parts of the text. The email content is as follows:

From: UITS Help Desk <support@email.arizona.edu>  
Reply-To: "upgrading8@gmail.com" <upgrading8@gmail.com>  
Date: Wednesday, November 28, 2012 12:22 AM  
Subject: Dear Account Owner!!

Dear Account Owner,

This message is from the UITS@ University of Arizona Service to all our account owners. We are currently upgrading our data base and e-mail center. We are deleting all unused Account to create more space for new one.

To prevent your account from closing you will have to update it below so that we will know that it's a present used account.

Confirm Your Email Account Below,  
NetID:  
Password:  
Re-type Password:  
Date of Birth:

Warning!!! Email owner that refuses to update his or her Email Account, within 24Hours of receiving this warning will lose his or her Email account permanently.

Thank you for your Co-operation.  
Copyright© UITS@ University of Arizonal 2012. All Right Reserved


The callouts and their corresponding text are:

- 1**: Misspellings –support is misspelled in this email.
- 2**: "Reply to" is a gmail account, not an official UA email address.
- 3**: References legitimate organization, but this is publicly available information that can be spoofed.
- 4**: Instills a sense of urgency for the user to act - this is Social Engineering at its best.
- 5**: Legitimate emails will not ask you to reply with this type of information included in the reply.

# How about Scams?

- 419 Scams!
  - Named for the section of the Nigerian penal code involving the “Nigerian Prince” emails that used to make the round, they happen way more than with just Nigeria now.
  - Someone wants money sent to them and then will give you money for helping them.
  - The website “419 Eater” is all about scammers being lured into “proving” themselves, like carving this wooden Commodore 64.





# What about “low tech” crimes and social media?



- Burglary:
  - Photos or statuses from vacation, if shared publicly, show that a person’s home is ripe for breaking and entering.
  - (Pictured: Me breaking my own rule, posting a photo of a section of the Berlin Wall while at a conference.)
- Selling scams:
  - Can’t always trust marketplace ads on social media.







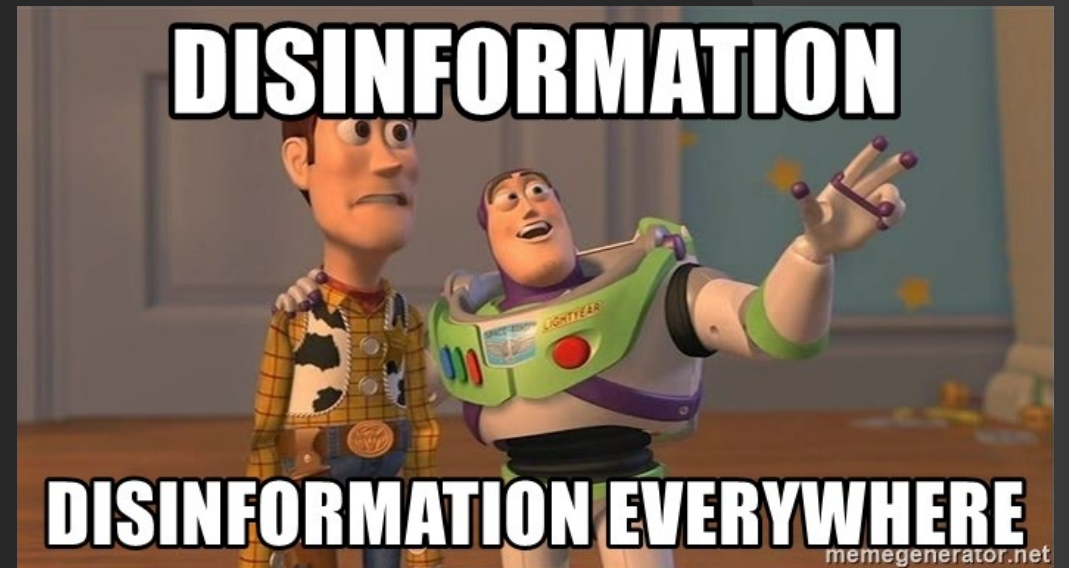
Oof...Disinformation...Oof.

- Two jokes to begin.
  - From the dawn of the internet:
    - There are three types of people in chat rooms: kids, predators, and FBI Agents. There are no kids.
  - From a more modern internet:
    - How do you tell the Russian trolls and bots from normal people? They speak better English than we do.



# Oof...Disinformation...Oof.

- The willful (or unwilling/unwitting) spreading of wrong information.
  - Social. Media. Is. The. Worst.
    - My beloved memes even.
- Often people will prey upon our worst beliefs about the “other” and spread stories to reinforce this.
  - Elections.
  - Tumblr sending out an “oops” sort of email about propaganda.
  - Sometimes things aren’t even really “disinformation” just provocative stuff.



# Cyberwarfare

The future is now...and has been.

When ALL approached me, Russia had not yet invaded Ukraine.

However, I still thought of when it invaded South Ossetia, when getting ready for this presentation...they started with widespread cyber attacks.

Then, about six weeks ago, 200,000 Russian soldiers poured into Ukraine...alongside massive cyber attacks.

# Cyberwarfare

Russia hit or engaged in the following in both cases:

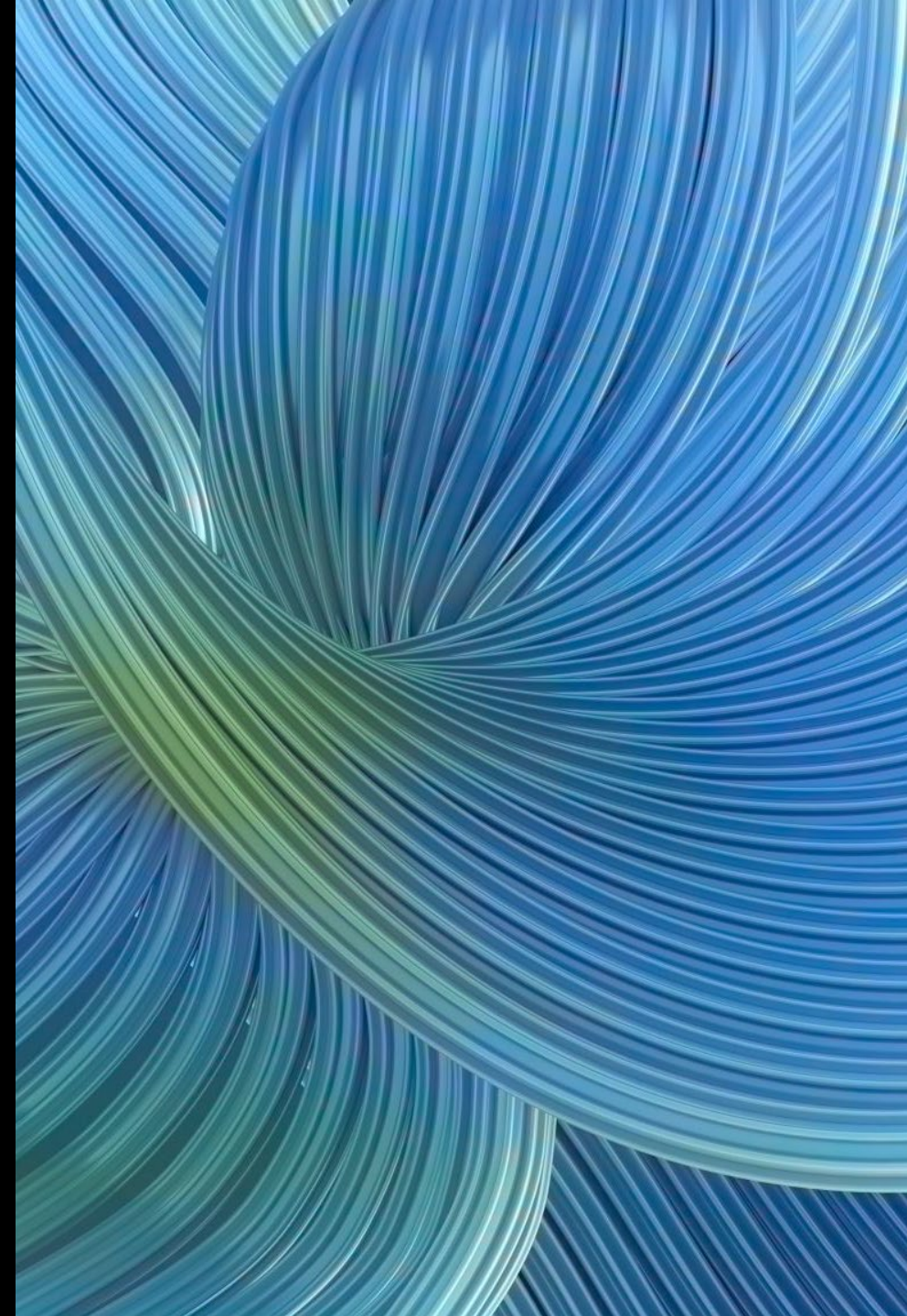
Disrupting official government websites.

Disrupting banking systems.

Disrupting air traffic control.

Spreading rumors about false troop movements.

Some are even now calling the war in Ukraine, “The TikTok War,” as people on the ground, and propagandists, produce videos on the widely used platform.



# Cyberwarfare

- Now that's all pretty scary...but, let's look at something the US government declassified.
- This is test footage declassified in 2016, but recorded in 2007.
- This generator is essentially destroyed with almost all internal parts needing replacements, without a single bullet being fired, only a few lines of computer code.



# One last topic...Deepfakes.

1984, "The party told you to reject the evidence of your eyes and ears. It was their final, most essential command."

I wish we didn't live in a world where I have to contradict Orwell's warning about being told to not believe your own eyes and ears, but here we are...

- The creation of videos or photos that go beyond photoshopping existing content into creating new disinformation.
- Imagine if we turn on the news and see, say, a former President talking about Scooby Doo, and how much we love Scooby Doo? Is he really doing it? Or is it something else?
  - <https://twitter.com/etienneshrdlu/status/1324674321336459264>
- This small clip was created by using Deepfake Lipsynch technology, an impersonator doing the voice, and a video (with audio removed) posted by a previous US President.
- Sure, it may seem funny, but...what if it was something besides Scooby Doo? What if one day, a world leader makes a newscast that leads to war...but never made the broadcast, and it was all fake?

# Conclusion

Reagan liked to say, “Trust, but verify,” and while the Soviet Union may be gone, it’s good advice for anything involving the internet.

Or in the words of fictional FBI Agent Fox Mulder, “Trust No One.”

Any thoughts, questions, comments, etc?

# Further Information Videos: Last Week Tonight with John Oliver: Ransomware





# Further Information Videos: James Veitch on Scamming a Scammer

- [https://www.ted.com/talks/james veitch this is what happens when you reply to spam email](https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email)
  - Apologies, the TED site doesn't want to cooperate with me on embedding it instead of just a link!

# Further Information Deepfake Article: When Seeing is No Longer Believing

- <https://www.rnz.co.nz/news/the-wireless/375262/deepfakes-when-seeing-is-no-longer-believing>
  - Discusses Deepfakes starting in pornographic content, then moving onward to politicians and disinformation campaigns about issues like mass shootings.