Why an April Update?

• The University System of Georgia and Kennesaw State University continue to be the target of malware, ransomware, and financial fraud attacks.
• To provide timely information to the campus community, ensuring our employees remain aware of timely threats.
• In alignment with the USG Bi-Annual training requirement, this is the first of a series of regular security updates.
Overview

• A closer threat examination
  • Ransomware
  • Spear Phishing
  • Financial Fraud
  • COVID 19 Scams
  • Remote Working Safeguards
• Summary and Key Points
• Additional Resources
Ransomware

- Ransomware is a type of malicious software, or malware
- Access to data or system is denied until a ransom is paid
- It spreads through phishing emails
- It also spreads from infected websites, known as drive-by downloading

Credit: https://www.us-cert.gov
Ransomware Attacks and Their Costs:

Attacks have a significant cost whether the ransom is paid, or we choose mitigation and recovery of data:

- Jackson County, GA in March 2019 – paid $400K ransom
- City of Cartersville, GA in May 2019 – paid $380K ransom
- City of Baltimore in May 2019 – over $18M in mitigation costs
- Various towns in TX (22) in August 2019 – over $12M in mitigation costs

Protecting Yourself from Ransomware

• Store your business-critical files on Microsoft OneDrive, or in the case of confidential data, on your departmental network share
• UITS centrally manages patches for university devices. If you're unsure whether your device is being patched, details are available on the UITS website linked at the end of this training
• Forward suspicious emails to UITS at abuse@kennesaw.edu or simply delete them
• Only install applications from trusted sources; If you're not sure, reach out to the Service Desk
• Practice safe web browsing:
  • Make sure a URL includes HTTPS before entering any personal information
  • Don't click on pop-up windows or extraneous ads
  • Use a strong, unique password or passphrase for each account, and avoid storing account information on a website
Spear Phishing

- Targets you by pretending to be your manager, co-worker, or some other person with whom you interact or know and trust.
- Spoofs an email to look like it is a legitimate request – always check the return address to verify the proper @kennesaw.edu address (watch for EXTERNAL in subject).
- Requests your help by using a compelling, fabricated story that is usually urgent in nature.
- Takes advantage of your pre-existing relationship with the person they are spoofing for their own gain.
Spear Phishing Example Part 1:

From: [Trusted Name] <fake_name@gmail.com>
Sent: Monday, March 4, 2019 4:54 PM
To: victim@kennesaw.edu
Subject: Are you on campus
Available?

Subject: Re: Are you on campus

I need you to help me get an iTunes Gift card from the store and send me pictures. I will reimburse you back when I get back to the office. I need to send it to someone and it is very important because I am still at the meeting and I need to get it sent as soon as possible. Today is my best friend's son's birthday.

Thanks!
Best regards.
Spear Phishing Example Part 2:

From: [Trusted Name] <fake_name@gmail.com>
Sent: Monday, March 4, 2019 4:59 PM
To: victim@kennesaw.edu
Subject: Re: Are you on campus

I need you to help me get an iTunes Gift card from the store and send me pictures. I will reimburse you back when I get back to the office. I need to send it to someone and it is very important because I am still at the meeting and I need to get it sent as soon as possible. Today is my best friend's son's birthday.

Thanks!
Best regards.
Spear Phishing: How Do I Spot It?

• Are you being asked to take action (go to a website, download files)?
• Are you being asked for money, gift cards, or a credit card number?
• Are you being asked for credentials (netID, password)?
• Can you verify the identity of the requester (is that an external address)?
• Is there a sense of urgency (I need it now, ASAP, I’m in a meeting)?
• Is the requester asking you to do something that doesn't make sense for your role?

STOP-THINK-CLICK!
Financial Fraud

• Billions of dollars are lost each year due to fraudulent transactions originating from spear phishing emails and counterfeit financial forms

• Over 23K complaints in 2019 to the FBI

• Human Resources and Payroll departments are frequently targeted in direct deposit change fraud

• Attacks are frequently low-tech (phone / fax / email) and circumvent technical security controls

Source: https://www.wsj.com/articles/email-scammers-are-savvier-and-more-successful-than-ever-11582808400
Financial Fraud – How do I help prevent it?

• Don’t assume an email or phone call is authentic – Verify!
• Unless you initiated the transaction, never give out your personally identifiable information (PII)
• Beware of IRS emails or texts requesting personal or financial information
• Awareness is the KEY to preventing attacks
COVID 19 Scams

Beware of:

• All robocalls, texts, and emails claiming to have home testing kits
• So-called Coronavirus "cures"
• Claims of a mandatory national two-week quarantine
• Offers to clean your HVAC ducts
• Charities (many are legitimate, but do your research!)

Source: https://www.fcc.gov/covid-scams
Some Sites to Avoid:

- coronavirusstatus.space
- coronavirus-map.com
- coronavirus-realtime.com
Protect Yourself Against COVID 19 Scams

• Get your information from a legitimate source
• Use your search bar to go directly to the CDC or World Health Organization’s websites
• Do not click on any link in an email that you aren’t 100% sure who the sender is
• Be aware, phony travel deals abound; when you’re on a travel site, check that the URL contains the lock icon, so you know it is secure
• Contact law enforcement if you believe you have been the victim of a Coronavirus scam
A COVID-19 Text Message Scam:

- CBC (Canada) News reported that there is a financial fraud text message.
- The text message appears to be from the Red Cross offering free face masks to every Canadian household.
- If you click on the link it takes you to a wholly unaffiliated website asking for your credit card info for a donation or for shipping fees.
Remote Working Tips:

• Beware of installing non-KSU-approved software on your work PC
• Encrypt email attachments containing confidential data
• Make sure your internet connection is secure by utilizing the KSU VPN (GlobalProtect)
• Keep your software up to date with the latest security patches
• Keep up good physical security habits of locking your screen
• Avoid storing personal information on issued systems
Data Sharing Options

• For sensitive and/or public information, use MS Teams and email.
• For confidential data (SSNs, driver's license, bank account, credit cards, Private Health Information (PHI), passports) use solutions architected to ensure security:
  • If you are emailing confidential information as part of your business process, encrypt attachments using https://jirafeau.kennesaw.edu
  • If you are storing confidential information, use the systems of record or restricted network shares (I:/ and M:/ drives)
• Reference: https://uits.kennesaw.edu/document-management/
Summary / Key Points

- **Beware** of emails or phone calls asking for money, gift cards, or with time limits
- **Avoid** installing any third-party software on your KSU devices
- **Bear** in mind the potential cost of the exposed risk to the organization
- **Forward** suspicious emails to abuse@kennesaw.edu
- **Don't be afraid to verify** when in doubt
- **Don’t panic!** Stop and think before you click
- **Secure** your remote workstation
**Additional Resources**

- KSU UITS Service Desk for Faculty / Staff: 470–578-6999
  service@kennesaw.edu
- If you mistakenly provided credentials to a confirmed phishing email, please change your NetID password immediately at [https://netid.kennesaw.edu](https://netid.kennesaw.edu)
- If you suspect an email, please forward it to abuse@kennesaw.edu
- Check the Phish Market for updated phishing information at [https://uits.kennesaw.edu/ocs/phish-market/index.php](https://uits.kennesaw.edu/ocs/phish-market/index.php)
- Check for IT system status first for updates on routine maintenance or outages at [http://status.kennesaw.edu](http://status.kennesaw.edu)
Thank You!

- Slides will be available at https://uits.kennesaw.edu
- Send any additional questions comments to ocs@kennesaw.edu