

# IT Security Awareness

Jake Coffman – Interim CISO



# Discussion topics



## Current Protections

What / how is KU protecting its community

Review technologies in place, their purpose and how they help you.



## Current security trends / attacks

What KU has seen in our threat landscape

Review of actual attacks and how KU leverages its toolsets to remediate and resolve.



## Cybersecurity Training

‘You are the shield’

Update on cybersecurity efforts and why they are important.



## At home protections

Resources, best practices in our digital realm.

We’re not going to undo what the pandemic (good and bad) has brought, we’ll need to manage it.



# Bitlocker / Filevault WDE

Whole disk encryption is used on KU managed devices



## Protects against loss or theft

Data is unusable in a case of loss or theft.



## Compliance

Meeting compliance standards for both state and federal.



# Microsoft Defender EDR

Microsoft Defender Endpoint Detection and Response is used on KU managed workstation.

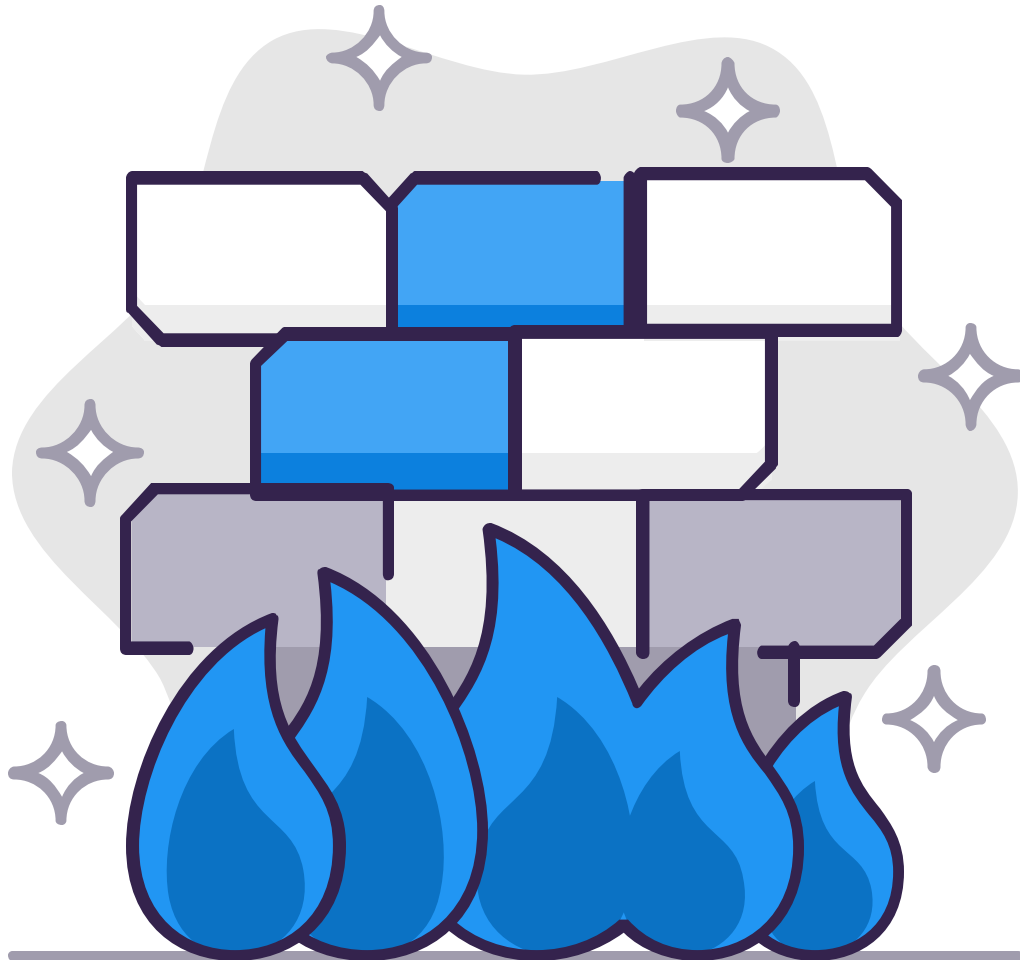


## Protections against malware and other anomalous activity

- ✓ Malware automation / remediation
- ✓ Ransomware detection and isolation
- ✓ Anomalous activity
- ✓ Vulnerability mitigation

# Firewalls and network protections

KU's network is protected by firewalls and other technologies



## Protections against common probing, identity matching

- ✓ Multiple firewall layers to protect our endpoints and other resources
- ✓ Known 'bad resources' are blocked
- ✓ Malicious URL's are unreachable
- ✓ Identity matching and resource access

# Cybersecurity training

KU partnered with SANS.org for training

## 'You are the shield'...but really, you are.

Majority of compromise happen on user-based activities; ie phishing, unsafe browsing, re-use of passwords etc.

Testing and training videos will be tailored to current themes and threats.



59%

2021  
Completion



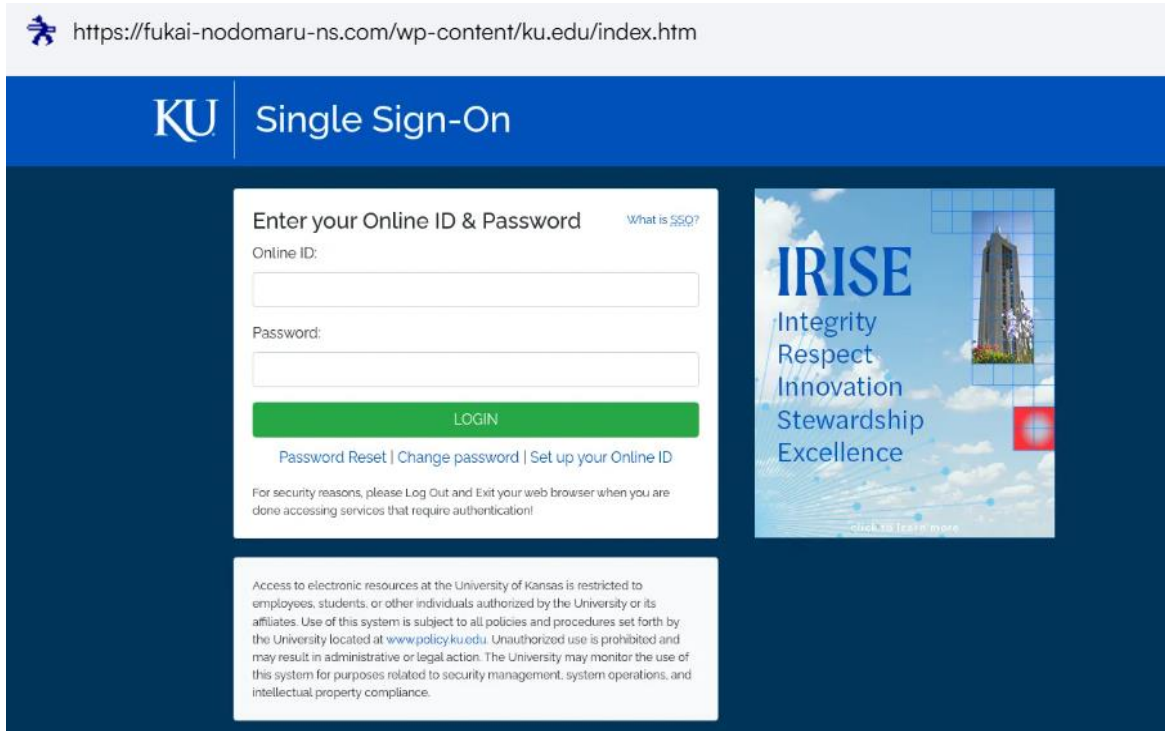
93%

2024  
Completion



# Phishing

Phishing is the easiest, lowest effort for entry



The screenshot shows a web browser address bar with the URL <https://fukai-nodomaru-ns.com/wp-content/ku.edu/index.htm>. The page has a blue header with the KU logo and the text "Single Sign-On". The main content area is dark blue and contains a white login box on the left and a graphic on the right. The login box has the heading "Enter your Online ID & Password" with a link "What is SSO?". It includes input fields for "Online ID:" and "Password:", a green "LOGIN" button, and links for "Password Reset", "Change password", and "Set up your Online ID". Below the login box is a security notice: "For security reasons, please Log Out and Exit your web browser when you are done accessing services that require authentication!". At the bottom, there is a paragraph about electronic resource access restrictions. The graphic on the right features the word "IRISE" in large blue letters, followed by the words "Integrity", "Respect", "Innovation", "Stewardship", and "Excellence" in smaller blue letters. It also includes a small image of a building and a red square with a white cross.

## Tailored attacks at KU

### Bad actors **\*do\*** target us

Hackers do and will continue to target KU. These are not 'spam' or 'junk', they are tailored attacks to gain leverage on KU resources



#### Use Duo MFA

While MFA is a line of protection, it is not 100%

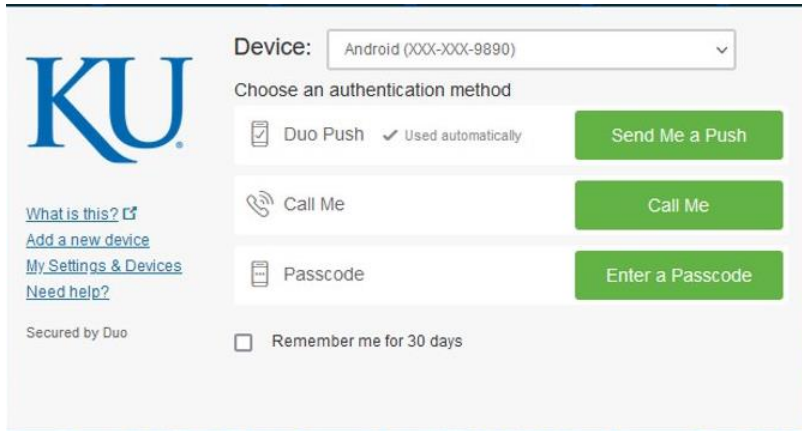


#### Vigilance and assurances on login pages

An attackers easiest method of entry is through credentials. Ensure wherever you're entering credentials in is safe.

# Phishing

(cont.)



## Tailored attacks at KU

### We do respond reactively / proactively

KU IT will respond once notified, either through toolsets or through the community and will also prevent these types of attacks



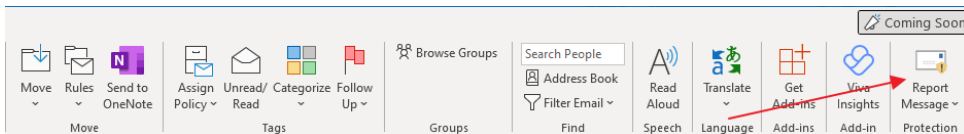
Email hygiene / email threat protection

Won't catch 100%, but will address most threats.



Report phishing, impersonation or other abusive email

Phishing emails can be reported to [abuse@ku.edu](mailto:abuse@ku.edu) or use the Outlook report messages button.





# Exposed infrastructure

From 0-day exploits, unmanaged websites etc

## 0-day exploits

Log4j response

Exposure of vulnerable systems. KU IT had to move quickly to resolve this high critical vulnerability.

## Un-upgradable equipment

Research leveraging non-standard / unsupported systems.

Research equipment, in general, has higher exposure and is more vulnerable to infection.

## Unmanaged websites

KU IT does not manage all websites

If you are managing your own websites, ensure appropriate updates are in place along with account security.

## 'IoT'

IoT is becoming more prominent

From raspberry pi's to temperature control units.



# Cybersecurity and vigilance at home

We need to be just as vigilant at home as we do at the office



## Secure IoT

Secure, update or even segment your IoT home devices.

## Secure home and personal devices, data and accounts



## Keep everything as up to date as possible

Update your home computers, devices, network hardware etc.

Secure the Family from SANS

<https://www.sans.org/mlp/secure-the-family/>



## Secure familial accounts

Ensure best practices are being used on shared, home accounts (bank accounts, Amazon etc)

ASUS router vulnerability

<https://www.bleepingcomputer.com/news/security/asus-warns-of-cyclops-blink-malware-attacks-targeting-routers/>



## Run antivirus

Run default Defender / don't disable inherent system protections

MFA as much as possible



## MFA, unique passwords, secure all accounts

MFA \*any\* account you may have; BestBuy, Steam, Facebook, Google etc.  
Use a password manager / unique passwords



# Also in the news...

(cont.)

## Esports league postponed after players hacked midgame

Lorenzo Franceschi-Bicchieri @lorenzofb / 10:39 AM CDT • March 18, 2024

Comment



## Social Engineering: How A Teen Hacker Allegedly Managed To Breach Both Uber And Rockstar Games

## CRACKING THE CODE

A negotiator says a 'bad day' is likely coming for K-State after cybersecurity breach

Chase Hagemann chagemann@themercury.com Jan 18, 2024

The New York Times



## Penn Data Breach Involves Decades of Student and Alumni Information

The hacker seemed focused on the Ivy League school's admissions preferences.

# Recent attacks

## Attacks using various methods



Social engineering

Phishing, impersonations etc.



0-day / software vulnerability

Cheats enabled mid-tournament via RCE



Supply chain

The product itself is infected.

# Fleeting thoughts

And other stream of consciousness.



## Keep in mind...

- ✓ Export control, collaborative work, travel etc:  
<https://gos.ku.edu/>
- ✓ Reach out in case of suspected malicious activity:  
[itsec@ku.edu](mailto:itsec@ku.edu) or [itcsc@ku.edu](mailto:itcsc@ku.edu)
- ✓ Ensure your data is safe by leveraging supported platforms:  
<https://technology.ku.edu/catalog/research-file-storage>
- ✓ Future of cybersecurity will change...

# THANKS!

Jake Coffman – Deputy CISO  
[jcoffman@ku.edu](mailto:jcoffman@ku.edu) – 785-864-0433  
[itsec@ku.edu](mailto:itsec@ku.edu)