

*Trojans Deceived.*

# Foundational Computer Security

July 21, 2023



macOS Monterey

Malware

Criminal Hackers

## List of malware types and what they do

But we don't have time to get into that, so just remember that malware is a collection of software-based tools that do bad things to you.

And criminal hackers use malware in addition to “social engineering” which are psychological techniques to influence your actions.

An example of both malware and social engineering is a phishing email, which encourages you to give away your secret information like passwords, credit card numbers, SSN, and/or entices you to execute some malware on your computer. They entice this through some urgent call to action or act of impersonation. We'll give some real examples later.

What you all can do to protect yourself is to practice your defense against these dark arts.

Updates, 2fa, being very careful before taking action on an email or message.


# Types of Malware



Type	What It Does
Ransomware	Disables victim's access to data until ransom is paid
Fileless Malware	Makes changes to files that are native to the OS
Spyware	Collects user activity data without their knowledge
Adware	Serves unwanted advertisements
Trojans	Disguises itself as desirable code
Worms	Spreads through a network by replicating itself
Rootkits	Gives hackers remote control of a victim's device
Keyloggers	Monitors users' keystrokes
Bots	Launches a broad flood of attacks
Mobile Malware	Infects mobile devices
Wiper Malware	Erases user data beyond recoverability.

Src: <https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/>



A close-up photograph of a light-colored wooden door. A hand is shown inserting a key into the lower part of a silver-colored metal door handle assembly. The upper part of the handle is a large, curved lever. The background is a plain, light-colored wall.

Close and lock  
all the doors and windows!  
(Apply security updates)

Installing Windows updates...  
Do not turn off your computer.

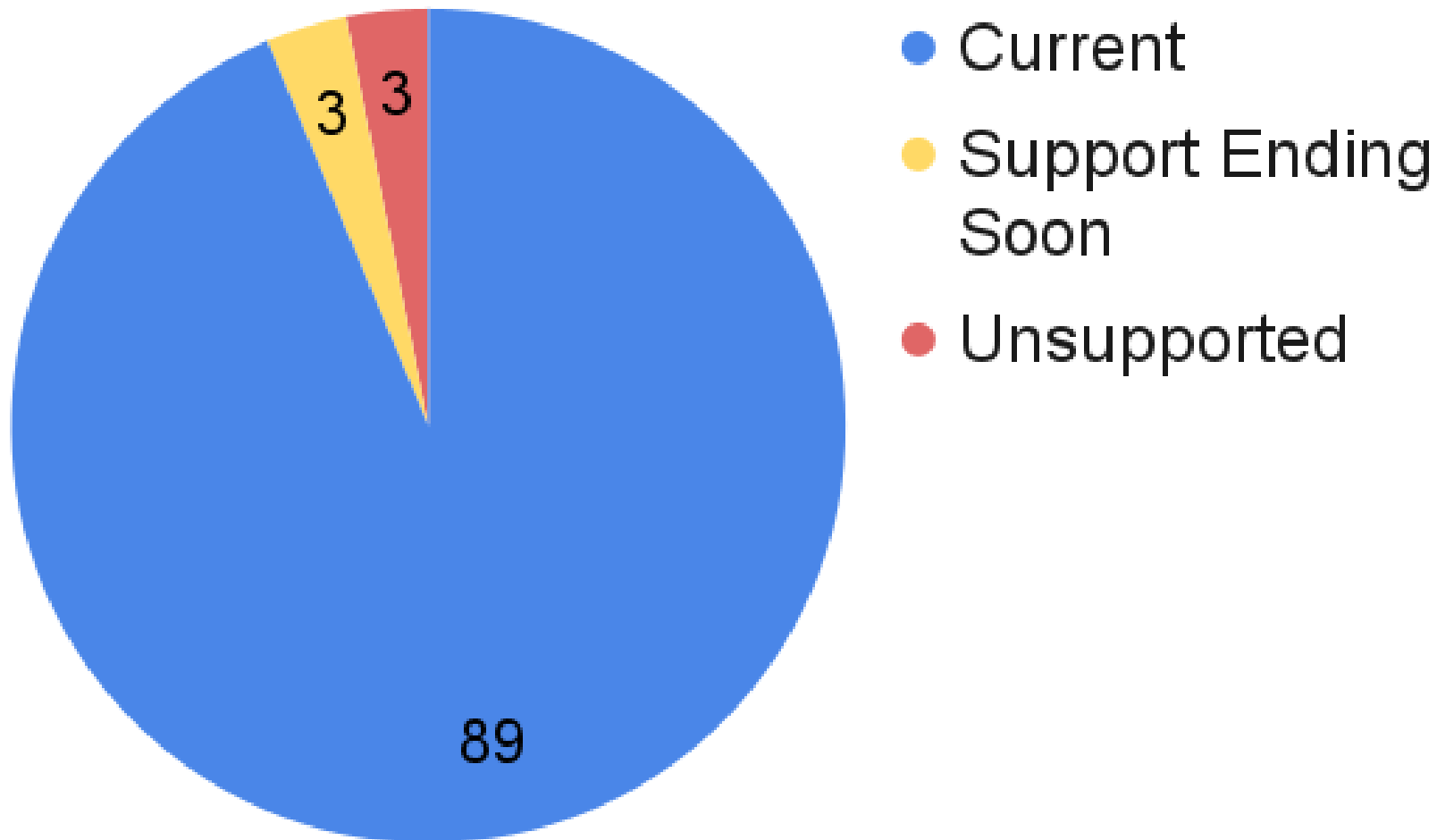


Installing macOS updates...  
Do not turn off your computer.

Patch all the vulnerabilities!  
(Apply security updates)

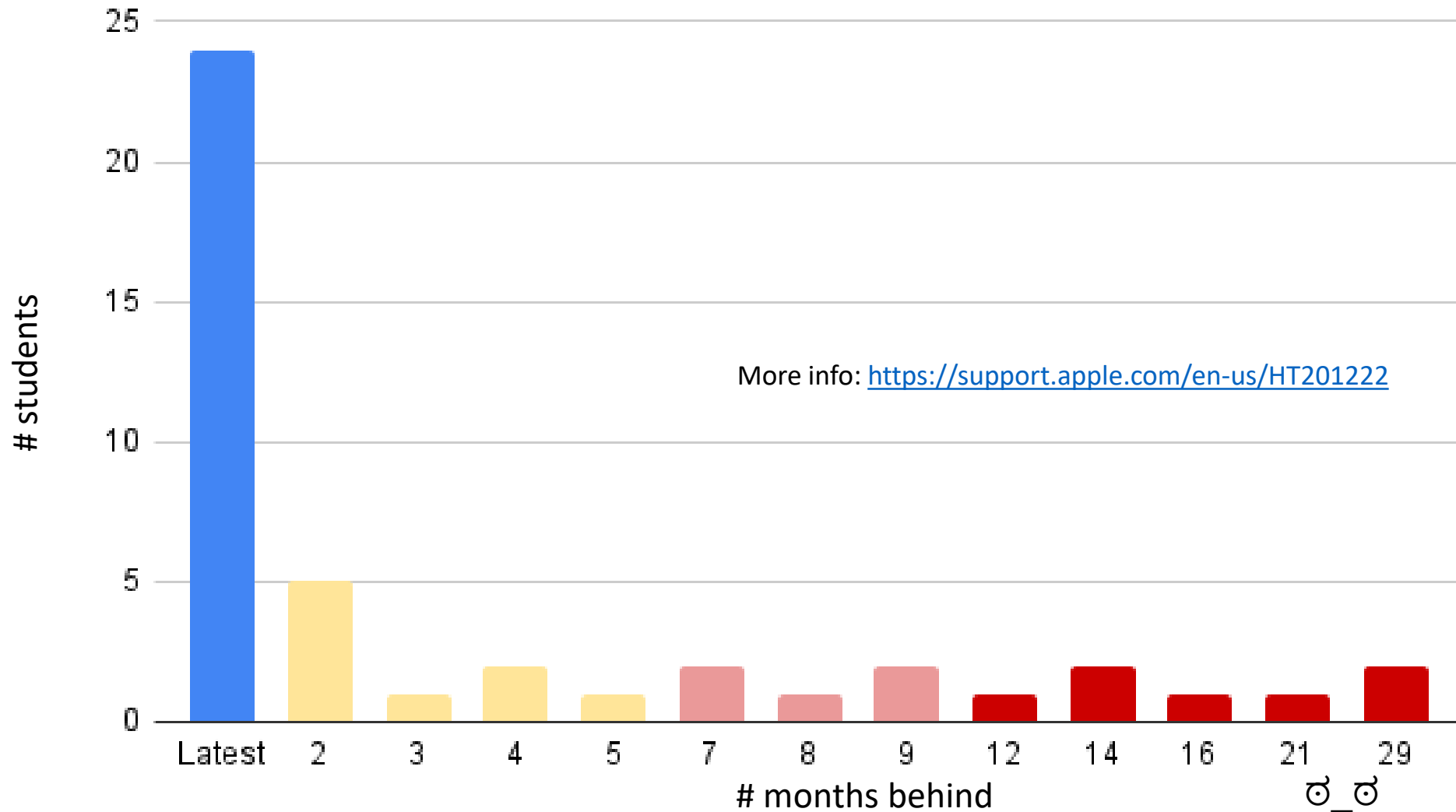
# MSA24 OS Version Survey Results

OS able to receive security updates?



# MSA24 OS Version Survey Results

macOS: # of months behind on security updates





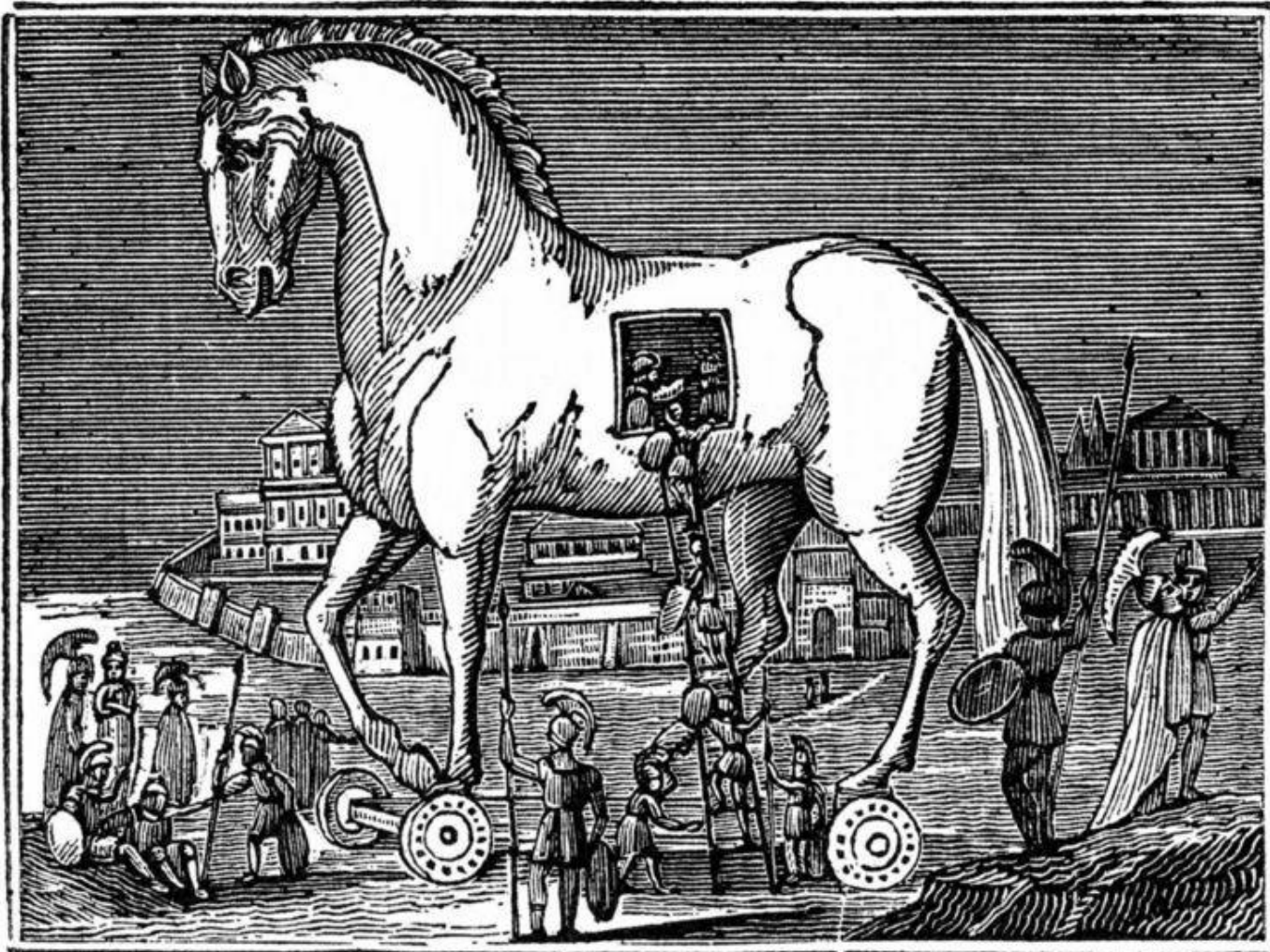


Hire a security guard!

Antimalware /  
Antivirus

- Realtime protection
- Periodic full scans

If your computer has malware, please meet with John to ensure disinfection.



*Trojans Deceived.*

- Your antivirus may only be aware of part of the malware.

# Helpful tools for malware defense

- <https://www.virustotal.com>

An AV aggregator. Upload a file (or a URL to a website) and it will scan it with 90 antivirus programs. Good for a “second opinion” on a suspicious file.

Caution: don't upload sensitive information.



# VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.





macOS Monterey

Malware

Criminal  
Hackers

# HOW ARE THEY GETTING IN?

Live Transcription (Closed Captioning) has been enabled

Who can see this transcript?



## Common Entry Vectors:

- Spear Phishing (90%)
- Social Engineering
- Credential Reuse Attacks
- Poor/No implementation of security controls
- USB/External Media
- Unverified or Insecure code dependencies

## Sophisticated Entry Vectors:

- Cloud compromises
- Compromising a 3<sup>rd</sup> party
- Compromising Managed Security Providers
- Internet of Things
- Zero Days

Source: FBI presentation on cybersecurity, no URL available



# Phishing Attempt

**U**te ex tunc cogitans, ut quoniam te ex tunc co-  
dignitatem hunc, ut quoniam ad dignitatem  
hunc dignitatem hunc, ut quoniam ad dignitatem  
hunc dignitatem hunc, ut quoniam ad dignitatem  
hunc dignitatem hunc, ut quoniam ad dignitatem  
hunc dignitatem hunc, ut quoniam ad dignitatem

**K**ite gaudet i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et

**V**egetus i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et

**S**ed i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et

**S**ed i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et

**L**et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et  
ambulatione p. et i. b. et ambulatione p. et i. b. et



## [Video – Phishing: Cyber Safety Series](#)

# Example Phishing Email

onlinestatements@email.estate Not a member

Your SunTrust mortgage billing statement is now available to view ([show original](#))



Dear SunTrust Client,

Great news! Your mortgage has moved to Online Banking at <https://suntrust.com>. Click [here](#) for details to help you get started.

Your SunTrust mortgage billing statement for your account ending with \*\*\*\*\*3193 is now available to view online.

To view your statement:

1. Visit [suntrust.com](https://suntrust.com)
2. Sign on with your Online Banking user name and password, or, create a new account by clicking "[Sign Up Now](#)"
3. Select Mortgage Loan from the My Accounts list

[whatcounts.com/t?r=62738&c=528&l=488&maid=19853434&ctl=5F:58AE6A865EEEF01B54CF73D2E83613EF6298549B](https://whatcounts.com/t?r=62738&c=528&l=488&maid=19853434&ctl=5F:58AE6A865EEEF01B54CF73D2E83613EF6298549B)

# Example Phishing Email

Check where the email came from. You may need to click “show original” to really see the sender’s address (thank you, Gmail...)

onlinestatements@email.estate Not a member

Your SunTrust mortgage billing statement is now available to view ([show original](#))



Dear SunTrust Client,

Great news! Your mortgage has moved to Online Banking at <https://suntrust.com>. Click [here](#) for details to help you get started.

Your SunTrust mortgage billing statement for your account ending with \*\*\*\*\*3193 is now available to view online.

To view your statement:

1. Visit [suntrust.com](https://suntrust.com)
2. Sign on with your Online Banking user name and password, or, create a new account by clicking "[Sign Up Now](#)"
3. Select Mortgage Loan from the My Accounts list

[whatcounts.com/t?r=62738&c=528&l=488&maid=19853434&ctl=5F:58AE6A865EEEF01B54CF73D2E83613EF6298549B](https://whatcounts.com/t?r=62738&c=528&l=488&maid=19853434&ctl=5F:58AE6A865EEEF01B54CF73D2E83613EF6298549B)

# Example Phishing Email

onlinestatements@email.estate Not a member

Your SunTrust mortgage billing statement is now available to view ([show original](#))



Dear SunTrust Client,

Great news! Your mortgage has moved to Online Banking at <https://suntrust.com>. Click [here](#) for details to help you get started.

Your SunTrust mortgage billing statement for your account ending with \*\*\*\*\*3193 is now available to view online.

To view your statement:

1. Visit [suntrust.com](https://suntrust.com)
2. Sign on with your Online Banking user name and password, or, create a new account by clicking "[Sign Up Now](#)"
3. Select Mortgage Loan from the My Accounts list

*Hover your mouse over links to  
see where they really go*

[whatcounts.com/t?r=62738&c=528&l=488&maid=198534348&ctl=5F:58AE6A865EEEF01B54CF73D2E83613EF6298549B](https://whatcounts.com/t?r=62738&c=528&l=488&maid=198534348&ctl=5F:58AE6A865EEEF01B54CF73D2E83613EF6298549B)



# Example Phishing Email

← → ↺

whatcounts.com/login.php?t=29ade33f8aff3213

Personal Banking

Small Business

Wealth Management

Commercial Corporate and Institutional

Search

Help Center

Open an Account

Sign On

Careers

Find Us

About Us



Banking

Loans

Retirement

Tools and Planning

Sign On

☐ Online Banking

☐ Online Cash Manager

User ID

Password

☐ Remember User ID

Sign On



PREPAID CARD

SUNTRUST

0000 1234 5678 9010

06/12 12/15

L. SCOTT

Debit

MasterCard

MORE CONVENIENT  
THAN CASH.

Never overspend again.

LEARN MORE ▶



**Upgrade Your Locks**  
**Use Multi-Factor Authentication**

# Multifactor Authentication Doesn't **Prevent** Phishing Attacks

## (But it helps!)



oit.ncsu.edu/2023/06/12/monkeypox-phishing-alert/?utm\_source=newsletter&utm\_medium=email&utm\_campaign=monkeypox-phishing-alert

June 12, 2023 | Featured, OIT News

## Monkeypox Phishing Alert

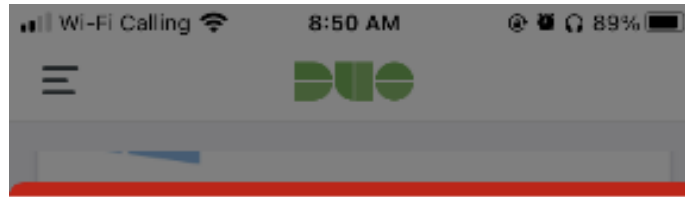
In mid-May, the university community was hit by two phishing attacks that allowed hackers to change several employees' direct-deposit information.

Both fraudulent messages warned campus employees of a "possible exposure to the monkeypox virus" and requested that the email recipient click on a malicious link to review information about a staff member with whom they might have had close contact.

Several recipients clicked on the malicious link and were directed to a fake NC State Shibboleth Login Service web page where they entered their Unity ID and password and then accepted a fraudulent Duo Security push. With the recipients' Unity credentials, phishers were able to log in to the MyPack Portal and change the recipients' direct deposit information; to stay undetected, the phishers then deleted the direct deposit confirmation email that was sent to the recipients' university Gmail account.

While the university continuously reviews its IT security measures and training, you remain its strongest defense against these types of attacks.

# Things to look for in a Duo 2FA Notification



Are you logging in to **NCSU**  
**SSL VPN?**

Requesting service

Geolocation of  
requester

🌐 **NC State University**

🕒 8:50 AM

👤 jajerni2



Deny



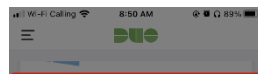
Approve

May 16, 2022 | Featured, OIT News

# Reject unsolicited Duo notifications

Be on the lookout for [multifactor authentication](#) (MFA) bombing — especially for unsolicited Duo Security notifications on your smartphone.

MFA bombing happens when an attacker bombards you with multiple account-access requests until you get tired of the annoyance and approve one in hopes of making it stop. After succeeding with one approved Duo request, the attacker then leverages that access to infiltrate additional MFA devices.



Weird?

Are you logging in to **Something Weird?**

● NC State University  
○ 8:50 AM  
▲ jajerni2



Was this a  
suspicious login?



Yes

No



# Ransomware: an Attack Strategy



**HACKER  
ENCRYPTS  
THE DATA**

**VICTIM SENDS  
THE PAYMENT**

**HACKER  
DECRYPTS  
THE DATA**





## Oooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

**Yes, You Can Recover All Your Files Easily And Quickly**

**But How ?**

**Send The Required Amount And  
I Will Send The Key To You For Decryption**

Your files will be lost on :

**71 : 58**

**See You Soon (0\_0)**

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



**Send \$100 worth of bitcoin to this address:**

1LHaSk425DzEoR6dT&6gc4wkoKnQ4iVwK

Copy

Show Encrypted Files

Decrypt

# Ransomware: an Attack Strategy

**HBO** ORIGINAL

LAST  
WEEK  
TONIGHT

WITH **JOHN OLIVER**

## PG-13 edit of Last Week with John Oliver – Ransomware

1. <https://www.youtube.com/embed/WqD-ATqw3js?start=0&end=346>
2. <https://www.youtube.com/embed/WqD-ATqw3js?start=374&end=594>
3. <https://www.youtube.com/embed/WqD-ATqw3js?start=666&end=1086>
4. <https://www.youtube.com/embed/WqD-ATqw3js?start=1106&end=1142>
5. <https://www.youtube.com/embed/WqD-ATqw3js?start=1152&end=1236>