UNC
SCHOOL OF MEDICINE

Cyber Security: Home & Work

Our Team – Who Are We?

UNC SCHOOL OF MEDICINE

- **2 IT Security Specialists**
(Peter Voland and Myron Morton)

- **1 Privacy Analyst**
(Tracy Wetherby Williams)

- **1 Director**
(Brian Penders)

We report to the SOM CIO and work closely with ITS-Security, the Institutional Privacy Office, and UNC Health ISD.

Cybersecurity in the News

UNC SCHOOL OF MEDICINE

UNC School of Medicine Reports 2018 Breach From Phishing Attack

NC: University of North Carolina at Chapel Hill School of Medicine and University of North Carolina Hospitals notifying some patients of breach

Two 'Russian' Ransomware Attacks Take Down North Carolina City And County Government Systems

UVM Health Network continues to tally costs of ransomware attack

Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.

Study reveals growing cybersecurity risks driven by remote work

Cybersecurity attacks surge as Ukraine-Russia war rages on. Here's how to protect yourself

4 Steps

UNC SCHOOL OF MEDICINE

4 Steps

UNC SCHOOL OF MEDICINE

1. **Implement multi-factor authentication** on your accounts to make it 99% less likely you'll get hacked.
2. **Update your software.** Turn on automatic updates so you don't have to remember to update manually.
3. **Think before you click.** More than 90% of successful cyber-attacks start with a phishing email.
4. **Use strong passwords**, and ideally a password manager to generate and store unique passwords.

https://www.cisa.gov/4-things-you-can-do-keep-yourself-cyber-safe

Implement Multi-factor Authentication – “Managed” Work Systems

UNC SCHOOL OF MEDICINE

- Today we will discuss strategies for securing both work and home systems. Many work devices are centrally managed.
- If you are unsure if a work computer is managed (typically using SCCM for Windows and Jamf for Macs), please check with School of Medicine IT to confirm: help.med.unc.edu.
- Important security settings are controlled centrally on managed work computers.

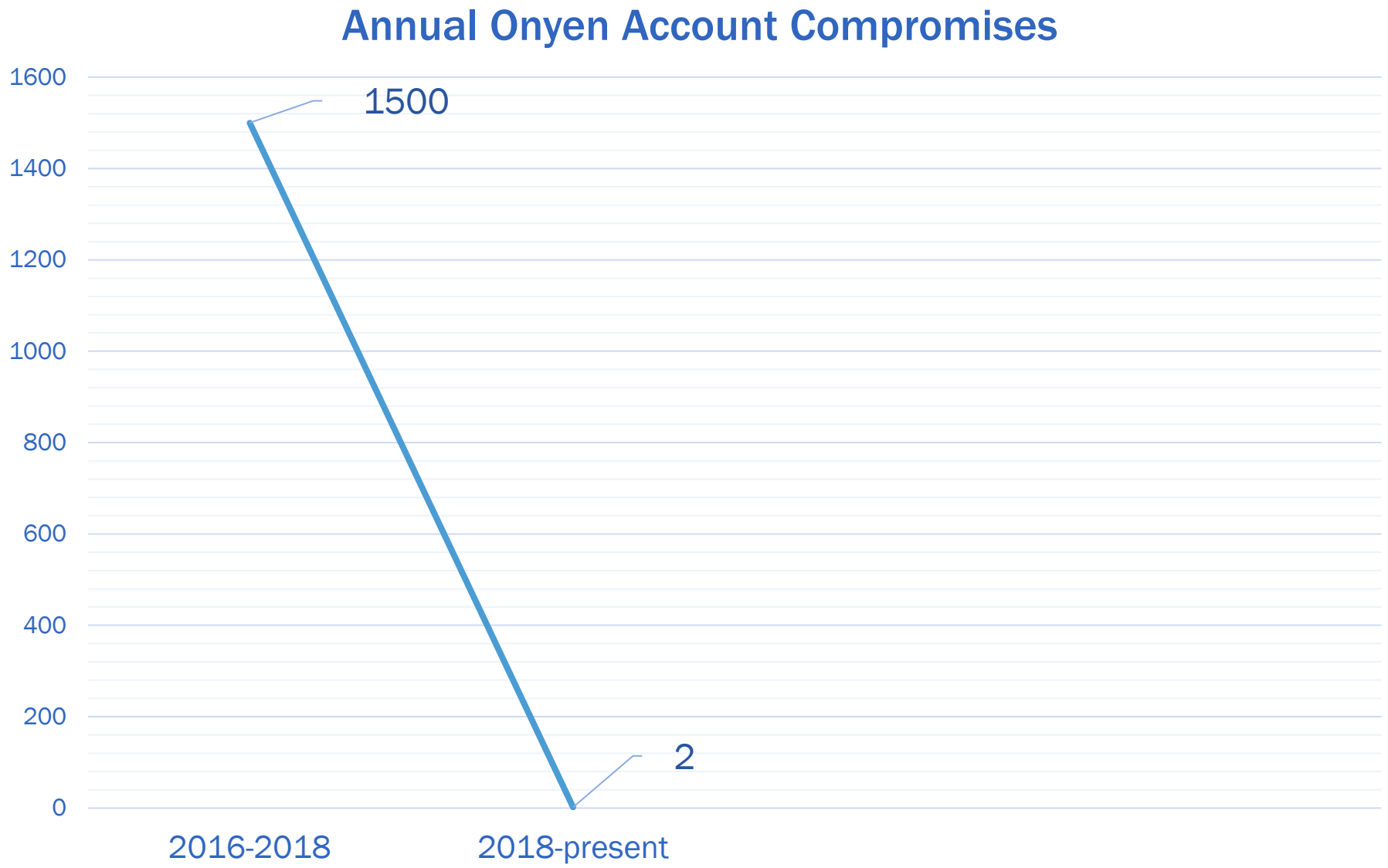
Implement Multi-factor Authentication – Good/Better/Best Practices

UNC SCHOOL OF MEDICINE

MFA Practice	Personal Accounts	Work Accounts
Good	Primary personal email account + Password manager (if used)	✓ Critical work accounts are automatically covered by Duo or Microsoft MFA
Better	Above + banking/finance accounts (i.e. bank/credit union, PayPal, Cash App, Venmo, etc.)	
Best	All Internet accounts where multi-factor authentication is available.	

Implement Multi-factor Authentication – Benefits

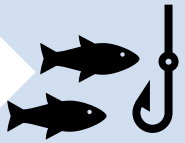
UNC SCHOOL OF MEDICINE



Timeline of Phishing Incidents

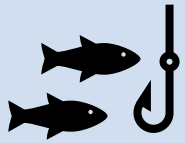
UNC SCHOOL OF MEDICINE

2016 Phish (W2s)



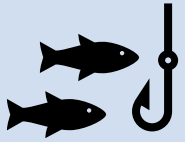
Wider Duo Rollout and M365 MFA Testing/Opt-in

2018 Phish (paycheck)



Full M365 MFA Rollout

2021 Phish (account gathering)



M365 A-5 Licensing

Update Your Software – Good/Better/Best Practices

UNC SCHOOL OF MEDICINE

Practice	Personal/Unmanaged System	Managed Work System
Good	Update software at least monthly	✓ Standard applications are updated automatically
Better	Update software at least weekly	
Best	Update software ASAP upon release/notification	

Think Before You Click

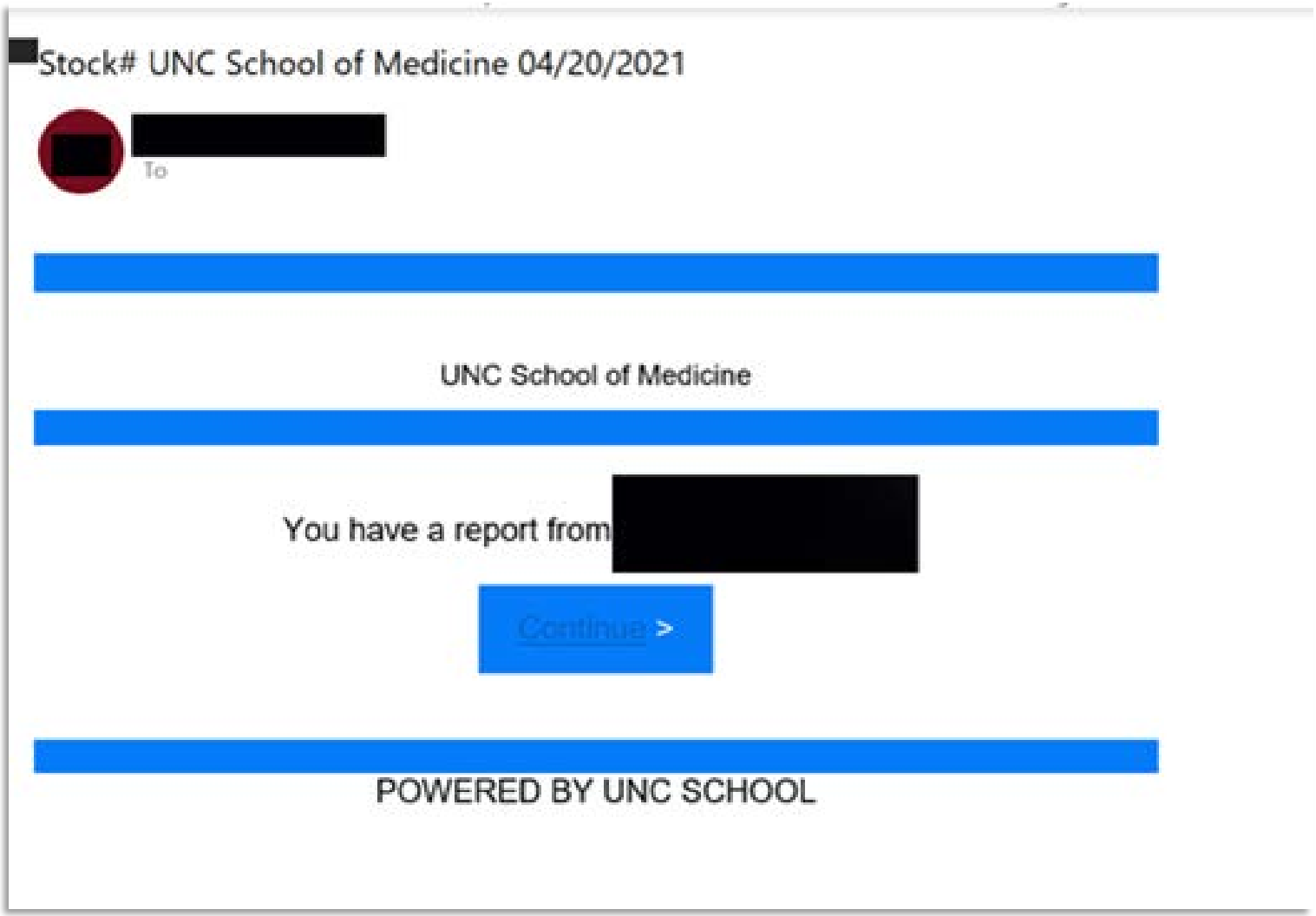
UNC SCHOOL OF MEDICINE

The threat of phishing/account compromise cannot be overstated.

- ✓ Be extremely vigilant when clicking links within email.
- ✓ Use caution when clicking links within Google search results.
- ✓ Let's discuss situational awareness at work…

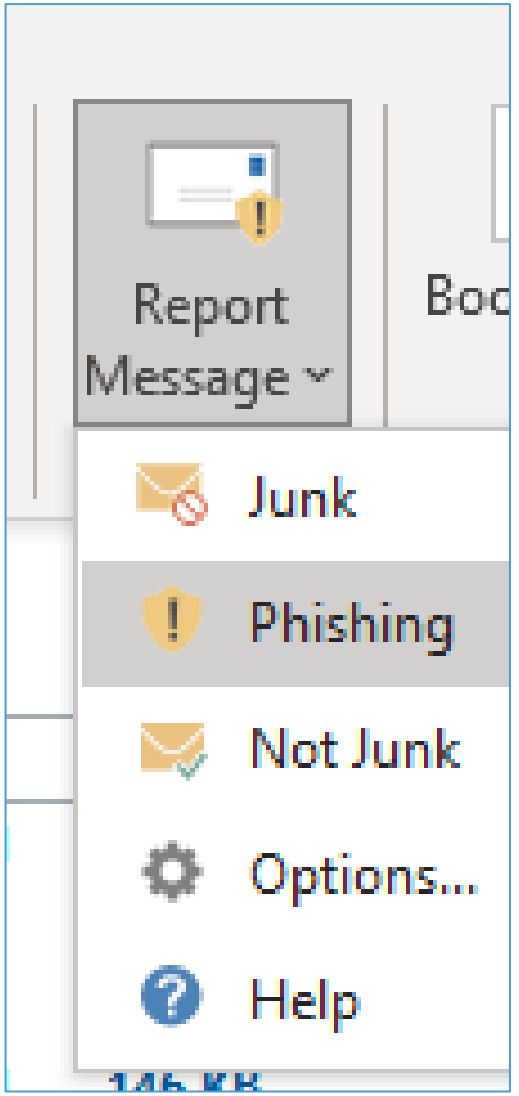
Think Before You Click - 2021 Phishing Incident

UNC SCHOOL OF MEDICINE



New Phishing Reporting Button

- The phish@unc.edu inbox has been decommissioned.
- New phishing reporting is available in all email applications (including phones) via an ellipsis (…), toolbar, or right-click option. Look for “Security Options” and/or “Report Message” then ”Phishing”.



Use Strong Passwords – Good/Better/Best Practices

UNC SCHOOL OF MEDICINE

Password Practice	Personal Accounts	Work Account
Good	Strong + unique password for primary personal email account	✓ Onyen password complexity is automatically enforced
Better	Above + include banking/finance accounts	
Best	Use of password manager – itself with strong + unique master password and multifactor authentication	

Use Strong Passwords – Password Manager

UNC SCHOOL OF MEDICINE

- Password managers are convenient and provide secure storage for all account passwords.
- UNC provides LastPass for free: https://lastpass.unc.edu or https://lastpass.com/partnerpremium/uncch.
- "But is a password manager too many eggs in one basket? If there's a breach, won't all my passwords be exposed?"
  - No. Password managers don't store your actual passwords. The passwords go through a one-way algorithm (hash) and are stored as a hexadecimal representation of the password.

Use Strong Passwords – Tips for Personal Accounts

UNC SCHOOL OF MEDICINE

- ✓ Consider passphrases.
- ✓ Avoid password reuse between accounts. Let's discuss…
- ✓ Avoid sequential password relation patterns, e.g. "Sleepy13!" => "B@shful14" => "Grumpy15#".
- ✓ For accounts that may be used infrequently or just once, consider a "throw-away" password; then use the password reset feature when needed.
- ✓ Avoid writing down passwords and leaving them visible near your computer in an area open to others.

Notes on Enterprise Data Management

UNC SCHOOL OF MEDICINE

- Take steps to understand the data classification of the information you work with every day.
- Ensure you are storing and sharing the above data appropriately.
- https://safecomputing.unc.edu/ is an excellent resource for UNC-CH data security.

We didn't discuss encryption, but managed work laptop systems **are encrypted.**

If your personal/BYOD system is encrypted, the system is only as secure as the login password/PIN.

Avoid using personal email for work-related communications.

Summary of High Level Tips

UNC SCHOOL OF MEDICINE

1. Protect your primary personal email account with a strong + unique password and multifactor authentication.
2. Consider a password manager for the convenience and security benefits.
3. Try to update your software at least monthly. We strongly recommend enabling automatic updates.
4. Be extremely cautious of links within email, and think twice prior to approving multifactor prompts.

Questions?

Direct contact via our group email: sominfosec@listserv.med.unc.edu or help.med.unc.edu.

Additional links from the slide deck:

- safecomputing.unc.edu/
- lastpass.com/partnerpremium/uncch

Thank you!