NCSA Security Talk for K-12 Teachers

James Eyrich
Manager NCSA IRST

Welcome! The presentation will begin shortly.

National Center for
Supercomputing Applications
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Disclaimer

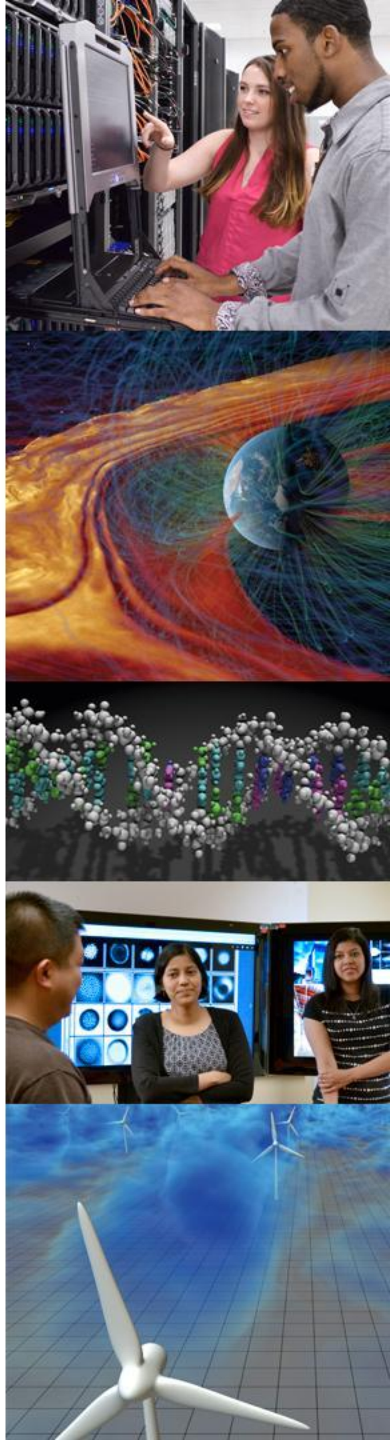
The information being shared is for educational purposes.

It is not meant to overrule your district's policies.

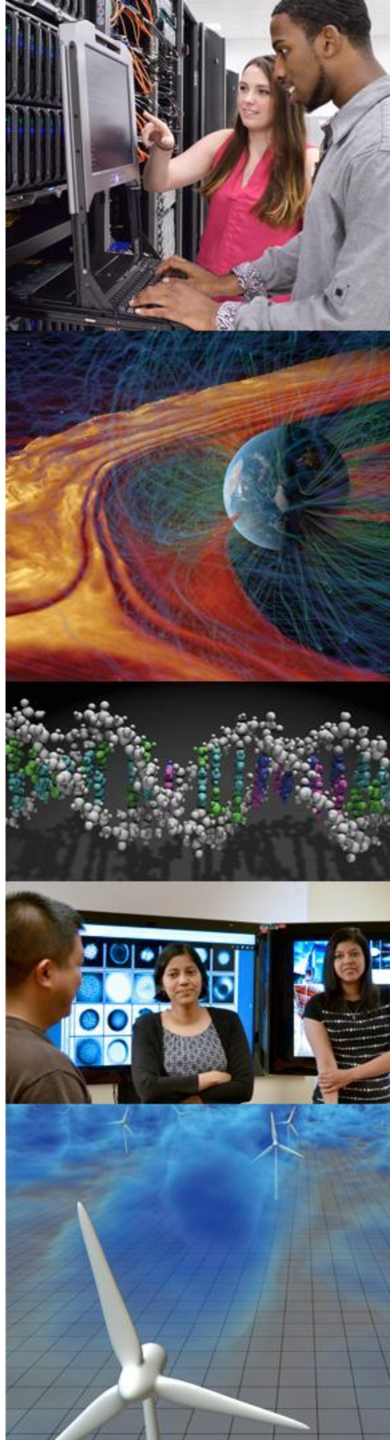
When in doubt, discuss with your IT department.

Outline

- Account and Password Hygiene
- Multi-Factor Authentication
- E-Mail Phishing and Scams
- Public Wifi Dos and Don’ts



Account and Password Hygiene



Account Hygiene

- Have a personal email account in addition to work provided
- Avoid mixing your work and personal email accounts
  - What happens after separation?
- Work account
  - May be subject to monitoring
  - content enforcement
  - Retention policies
- Personal account
  - You may cause it to become subject of FOIA or Discovery
  - Violating work policies
  - Nice to not see work stuff in your personal account - ie on vacation.

Avoid 3rd party Single sign-on (SSO)

- What is Single Sign-On
  - Allows you to log into one system and be automatically logged into others
- Examples
  - Enterprise Systems (Google Workspace, Microsoft Azure)
  - “3rd party” - Login with Facebook, Google, Apple...
- Concerns when using 3rd party
  - What happens if you lose access (FB jail) or disable your SSO account?
  - Do you trust 3rd party to not allow someone else into your other accounts?
    - 2018 Facebook had a data breach of 50 Millions accounts including SSO tokens.
  - 3rd party stops offering service
    - 2020 Apple announced it would no longer allow Epic users to sign in with Apple.
  - Tracking

Password Hygiene

- Random - real random, use a generator
- Long - the max allowed by the site, although no real need for more than 31.
- Do not reuse passwords

Do not let people watch you type a password

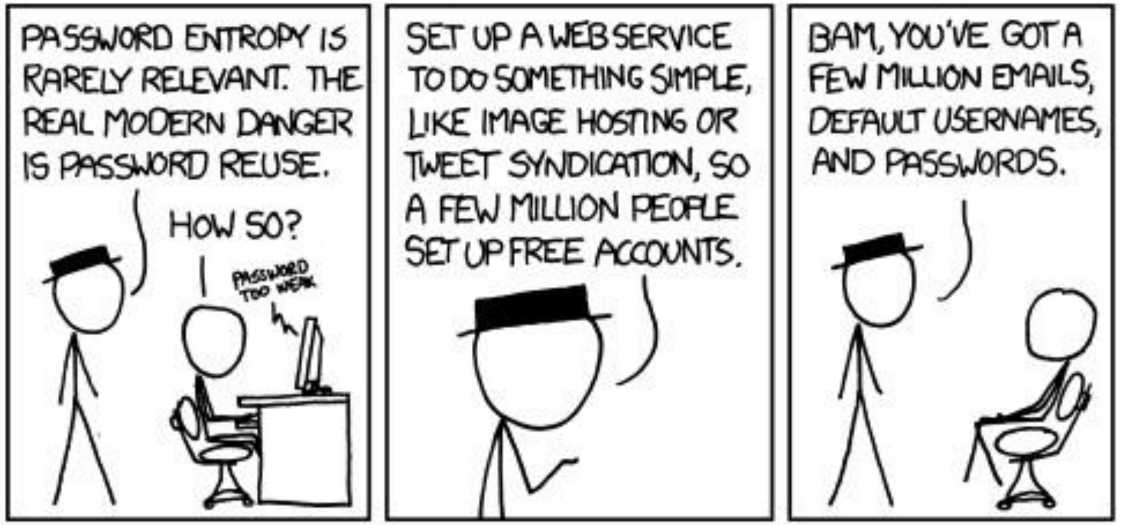
Safe Passwords

- Use different passwords for EVERYTHING
  - Use 14 char or more random passwords
  - Multiple character sets
  - Upper, Lower, Numbers, Symbols
  - The longer the fewer character sets needed

Safe Passwords - Exceptions

- Only use memorable ones for a few important things
  - District email/Apps account
  - Personal Email
  - Desktop/Laptop account
  - Amazon - ☺
  - password manager

Why Not Reuse Passwords?


PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.
HOW SO?
PASSWORD TOO WEAK
SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.

- Bad websites
- Hacked websites
- Exposed account details

Why Not Reuse Passwords?, cont.

haveibeenpwned.com

- Enter any email address you use
- See if your account info was leaked

Password Managers

- Paper
  - Better than reuse
  - Effective if you generate truly random passwords
  - Must keep on person, must protect
  - In general protecting from Internet not a mugger/thief
- Browser Built-in
  - New features for creating random passwords
  - Better than password reuse
  - Getting better - Sync / Local protection
  - Think twice before clicking “yes” to saving into the browser

Password Managers, cont.

- LastPass
  - Personal - free vs paid, many features now in free
  - Family Accounts
  - 2 factor
  - Allows Sharing to groups
  - Enterprise - push out policies (free Family with each lic)
- Others - cloud
  - Dashlane
  - 1Password
  - BitWarden - open source - also can host your own
- Others - offline
  - Keepass

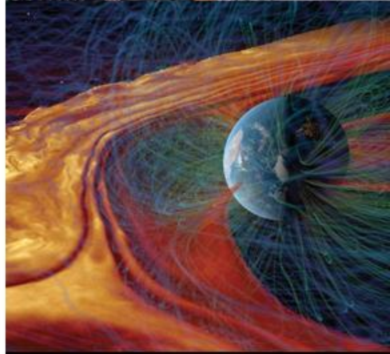
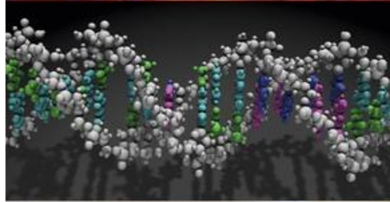
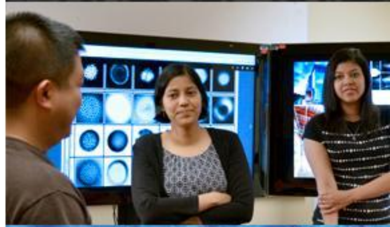
At least do this…

Create strong, separate passwords for your email, bank and mobile phone accounts.

Questions on account and password hygiene?

Multi-Factor Authentication

- Why it is important
  - Additional protection, even against an unknown breach
  - Requires an interactive component, as opposed to offline password hacking
- Why it is used in banking, healthcare, etc.
  - Same reasons as why I said at least pick strong unique passwords for bank, cellphone, email. Put the best security in front of the most important things.
  - Should also be used with an Enterprise SSO system

Multi-Factor Authentication

When possible enable multi-factor authentication.

aka MFA or 2FA

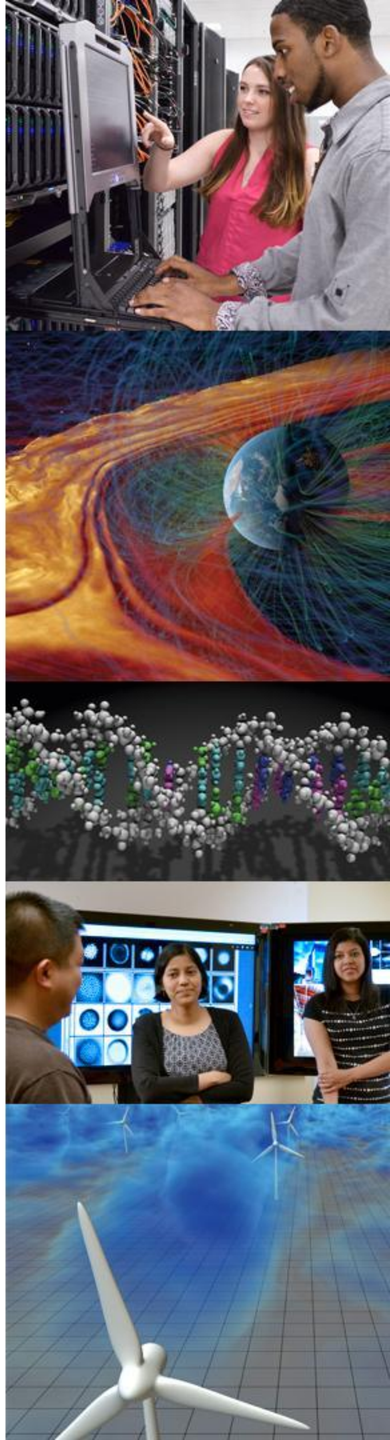
Two factor Auth Org - https://twofactorauth.org/

MFA examples - roughly in order of strength

- SMS code
- Email code
- Token - $20 U2F on Amazon
- Extra questions
  - sort of, is something you know, and maybe something everyone one knows.
- Google Authenticator - make sure you backup
- DUO
- RSA SecurID

Questions on multi-factor authentication?

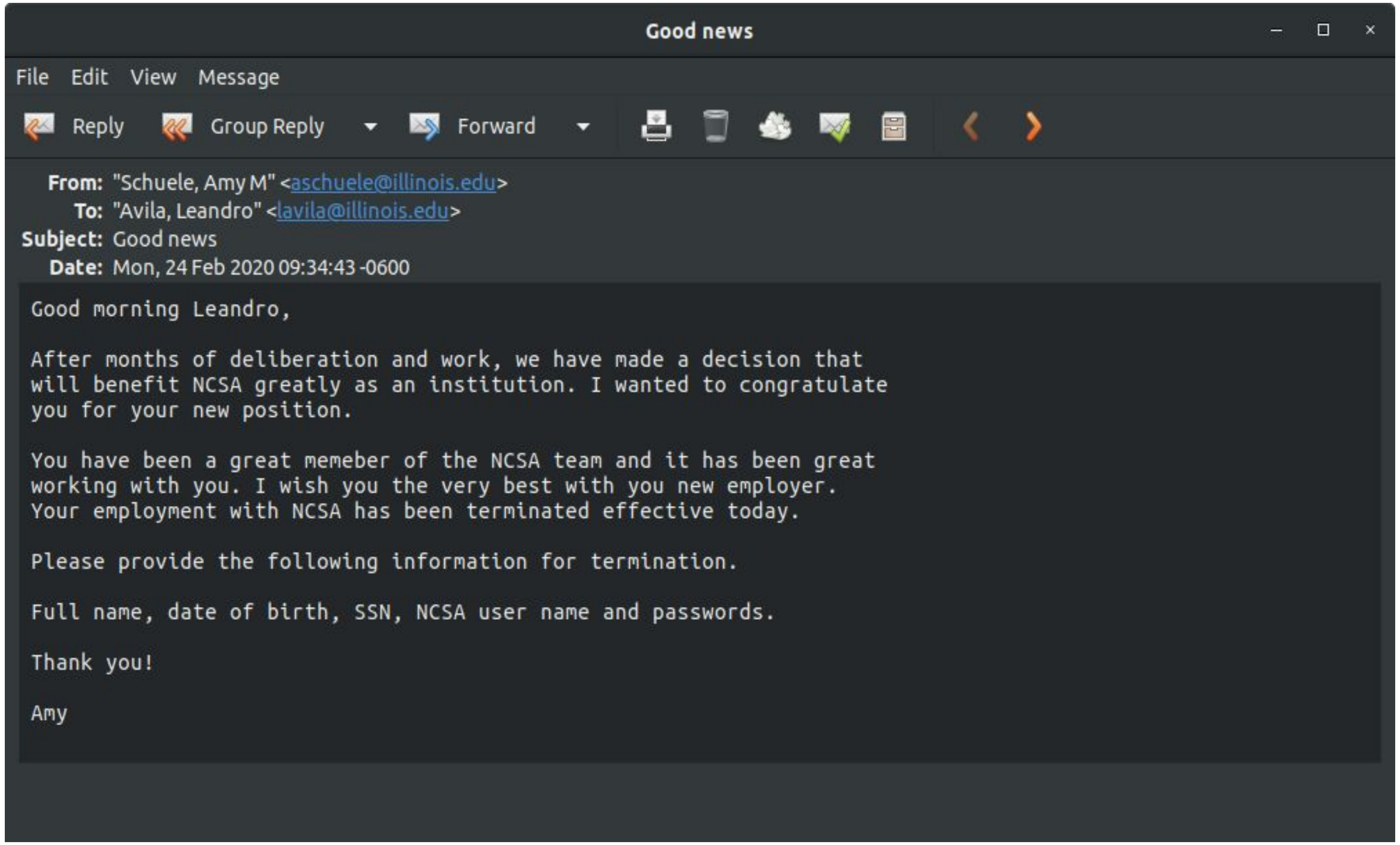
Email Phishing and Scams



Phishing

- E-mail most common point of entry for malware
- Most clicks shifting to mobile devices
- Be aware of SMS-based phishing
- Always be skeptical (ABS)

Phishing, cont.



From: "Schuele, Amy M" <aschuele@illinois.edu>
To: "Avila, Leandro" <lavila@illinois.edu>
Subject: Good news
Date: Mon, 24 Feb 2020 09:34:43 -0600

```
Good morning Leandro,

After months of deliberation and work, we have made a decision that
will benefit NCSA greatly as an institution. I wanted to congratulate
you for your new position.

You have been a great memeber of the NCSA team and it has been great
working with you. I wish you the very best with you new employer.
Your employment with NCSA has been terminated effective today.

Please provide the following information for termination.

Full name, date of birth, SSN, NCSA user name and passwords.

Thank you!

Amy
```

Always be skeptical.

If in doubt ask tech support.

Do not click or reply

Phishing, cont.

- Never send private information over email
  - Passwords, SSN, ePHI, Financial
- If you are not expecting the message be suspicious
- Look carefully at the details of the message
  - From address, spelling, etc
- If in doubt call or send a message via Skype/Slack

Gift Card Scams

You are contacted by someone impersonating your boss/coworker/family/etc.

They ask you to buy gift cards and send them the information because they need it **quickly**.

Gift Card Scams, cont.

- Gift Cards are like cash
  - If you do not do it with cash, do not do it with gift cards
- Urgency of the request is usually an indicator that something is wrong
- A variation of this will be to wire money

Remote work

Remote work makes it easier for some of these scams to occur.

Any purchases during remote work should be processed through some sort of authenticated system or verified by voice/video chat.

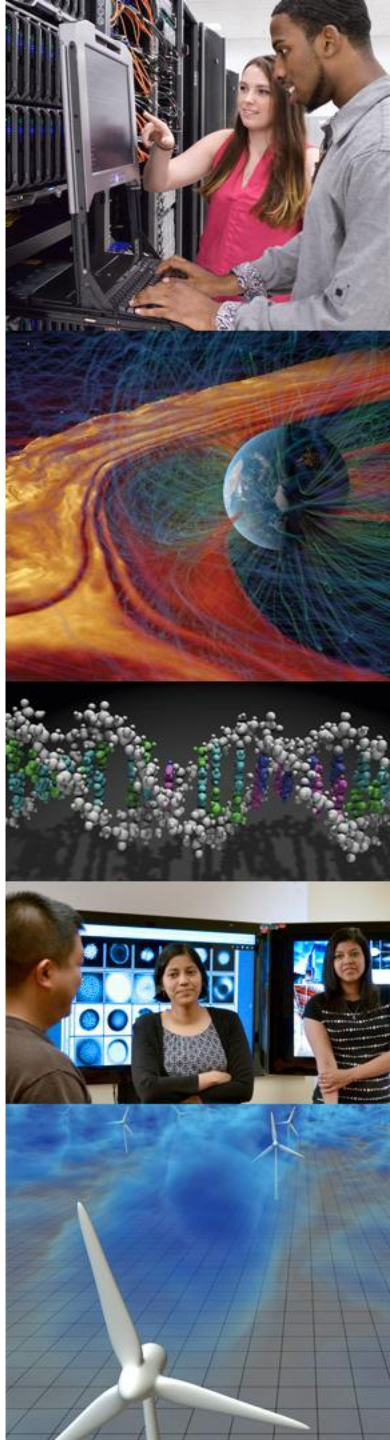
Always Be Skeptical

Questions on email phishing and other scams?

Using public WiFi

Public WiFi, district WiFi, cellular data – what’s the difference?

- Publicly available network connectivity.
  - It doesn’t matter if its open/closed wireless, or cabled.
    - Coffee shop, hotel, school, your friends
- Open vs Closed
  - Key/password needed or not, on older systems key did not protect from other users.
  - Newest standard allows for open to opportunistically encrypt (OWE) the connection.
- Cellular - is interceptable, your phone can be tricked into using a dirtbox (DRT)/stingray instead of a real tower.



Dos and Don’ts of public WiFi

- What business is it safe to conduct on public WiFi
  - Pretty much anything in 2022. Almost the entire Internet moved to using HTTPS after attacks like Firesheep and Snowden revelations.
  - As long as the URL is not something you need to keep secret.
    - But even DNS is being moved to encrypted from the browser. DoH(DNS over HTTPS),Private DNS
    - Firefox defaulted users in US to using DoH in 2020
- How do I know a website is secure
  - HTTPS protocol - the padlock symbol
    - But that doesn’t mean it’s to be trusted, just has a correctly signed certificate.
      - Certs are now free to get
      - Typo squatting
- What **not** to do when using public WiFi
  - Anything not encrypted or extremely sensitive (should it be anonymized?)

Questions on using public WiFi?

Thank you for attending!

Any more questions?

What did we miss?

Where to find us

Blog post with slides and video (when published):

https://wiki.ncsa.illinois.edu/display/cybersec/2022/07/25/Register+Now%21+Security+Talk+for+K-12+teachers

Website: security.ncsa.illinois.edu

Twitter: @NCSASecurity

About NCSA & CSND

The National Center for Supercomputing Applications (NCSA) provides computing, data, networking, and visualization resources and expertise that help scientists and engineers across the country better understand and improve our world. NCSA is an interdisciplinary hub and is engaged in research and education collaborations with colleagues and students across the campus of the University of Illinois at Urbana-Champaign and throughout the United States.

The Cybersecurity Division at NCSA is composed of researchers, developers, and specialists who work to advance the state of the art of cybersecurity, apply those advances to key science and engineering user communities, and provide for the high-performance and security of NCSA's networks and substantial computing resources.