



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE



Cybersecurity Overview for UAHRA

May 18, 2022

Wendy Worlund

Jeremy Shelley

Office of Information Technology (OIT)

Why Should I Care about Cybersecurity?

How do you use the Internet today?

- Email
- Financial Management - online banking, checking your investments and retirement accounts
- Research - news, recipes, home improvement or gardening tips (Pinterest)
- Online Shopping
- Social media (Facebook, Instagram, LinkedIn, etc.)



Why Should I Care about Cybersecurity?

- If you use email, text or the Internet at all, the chances are good that you've at least received a spam or phishing message
- Many scammers target Americans ages 65 and older
- Attacks via emails and websites for charitable donations, and health care
- Some are very tricky and well-executed
- Protect yourself, your data, and finances



Passwords



- Use strong passwords with eight characters or more that use a combination of numbers, letters, and symbols
- Mnemonics can help you remember them
- Don't use the same password twice; have a different password for every system just in case one is compromised

Multiple Factors, Not *Just* a Password

- Multi-factor authentication (MFA)
- 2FA (for two-factor authentication)
- Decreases risk of your account being accessed by someone else



Protect Your Devices

- Guard it as you would the cash it cost
- Install antivirus software and keep it updated
- Password or passcode on every device



McAfee®



Online Scams



Rather than clicking a link or responding to an email or text, visit the business's website or call them directly. You can verify information directly from the company by calling their published support number.

You can also hover over a link to see where the link would take you (rather than clicking it). If it would take you somewhere else, beware!

Online Scams



Websites and “from addresses” of emails can be spoofed. Bad actors may duplicate a legitimate website and direct you to it. When you try to log into the site, you’re giving them your username and password.

Check the email address, not just the display name. Spoofing scams use a sender name that will look familiar to try to trick you into opening the email and following the instructions. Whenever you get an email, hover your mouse over the contact name and look at the actual email address. They should match or be pretty close.

Online Scams



Callers can be very forceful and pressure you to take action immediately and try to stress you out about a situation being urgent that they're trying to *help* you before you lose more money, etc.

Don't let them waste your time and pressure you.

Take down the details of what they're reporting and hang up. Reach out to the source or just contact someone you trust.



Phishing and Spam

- Phishing is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.
- Spam is unsolicited email (junk mail). Usually, they want to sell you something.
- This is happening via text as well as email now.



Spam Example

[External] Wendy, shred prices with Shred-it (25% off enclosed)



External Inbox x



Shred-it Lynn.brown@shredit.com [via bounce.s10.mc.pd25.com](#)
to wendy.worlund ▾

Tue, May 10, 11:17 AM (7 days ago)



Having trouble reading this email? [View Online](#)

The banner features the Shred-it logo (a stylized 'S' made of three horizontal lines) and the text 'Shred-it® A Stericycle® Solution'. Below this, it says 'GET 25% OFF*' in large white letters on a blue background, followed by 'on your one-time paper shredding service.' and a yellow 'Learn More' button. The background of the banner shows a close-up of hands shredding paper.

Hello Wendy,

With Shred-it's one-time shredding services, 100% of the paper is destroyed safely and securely to prevent information security risks. Shred-it's service of-the-art security, a secure chain of custody with [barcode scanning at all touchpoints](#), and

- ← Reply
- Forward
- Filter messages like this
- Print
- Delete this message
- Block "Shred-it"
- Report spam
- Report phishing
- Show original
- Translate message
- Download message
- Mark as unread

Phishing Example

[External] The UAH Administrator has requested you view a meeting recording



External

Inbox x



Meeting Recording Bot recording@uah-meetings.com via psm.knowbe4.com
to me ▾

8:39 AM (16 minutes ago)



Dear Rae

You now have access to a new meeting recording that UAH has made available to you for your convenience.

Use the link below to access the meeting recording.

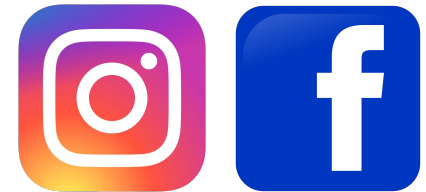
[Go to recording](#)

This link will expire on March 10, 2022.



Social Media Can Be a Dangerous Place

- Choose your friends carefully
- Use strong privacy settings to keep your information from being seen by strangers
- Don't overshare (wait until you're home from vacation to post those pics)
- Be careful what you click (just like with email and text)
- Report abuse



Identity Theft and Fraud

- Fraud - the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right
- Identity theft - the illegal use of someone else's personal information in order to obtain money or credit

Tips:

- When making online donations, vet the charity and make sure the website is `https://` instead of `http://`
- Shred bank and credit card statements before throwing them in the trash
- Check your bank and credit card statements monthly for unusual charges



If You Need Help, Ask for It

- Have a trusted person to speak with before responding to questionable messages
- There are many online resources available to seniors
- If you need UAH's Office of Information Technology, contact the OIT Help Desk through one of these channels:
 - Our Client Portal - uah.edu/ithelp
 - Email - helpdesk@uah.edu
 - Phone - 256-824-3333

