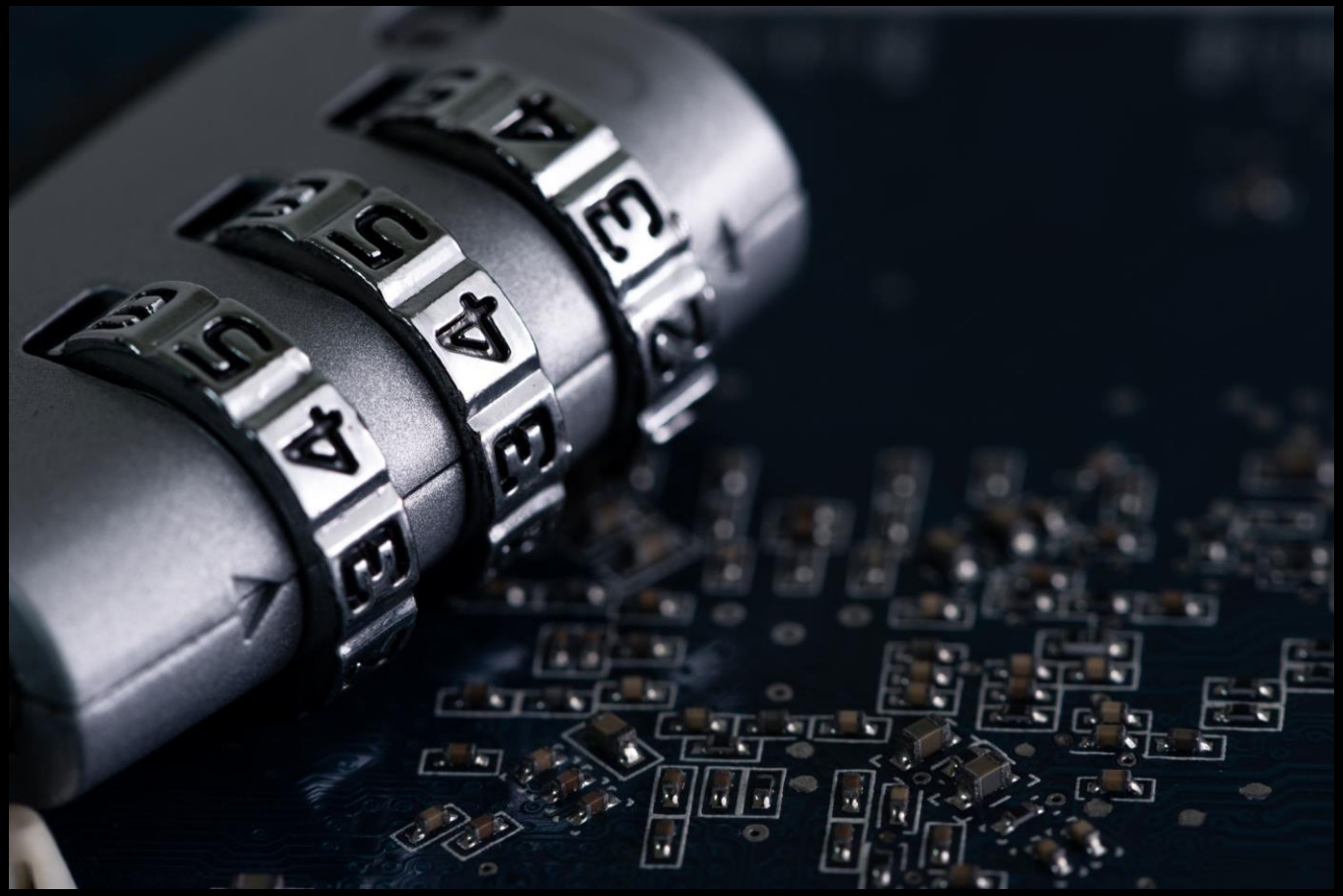
Security Essentials for End Users

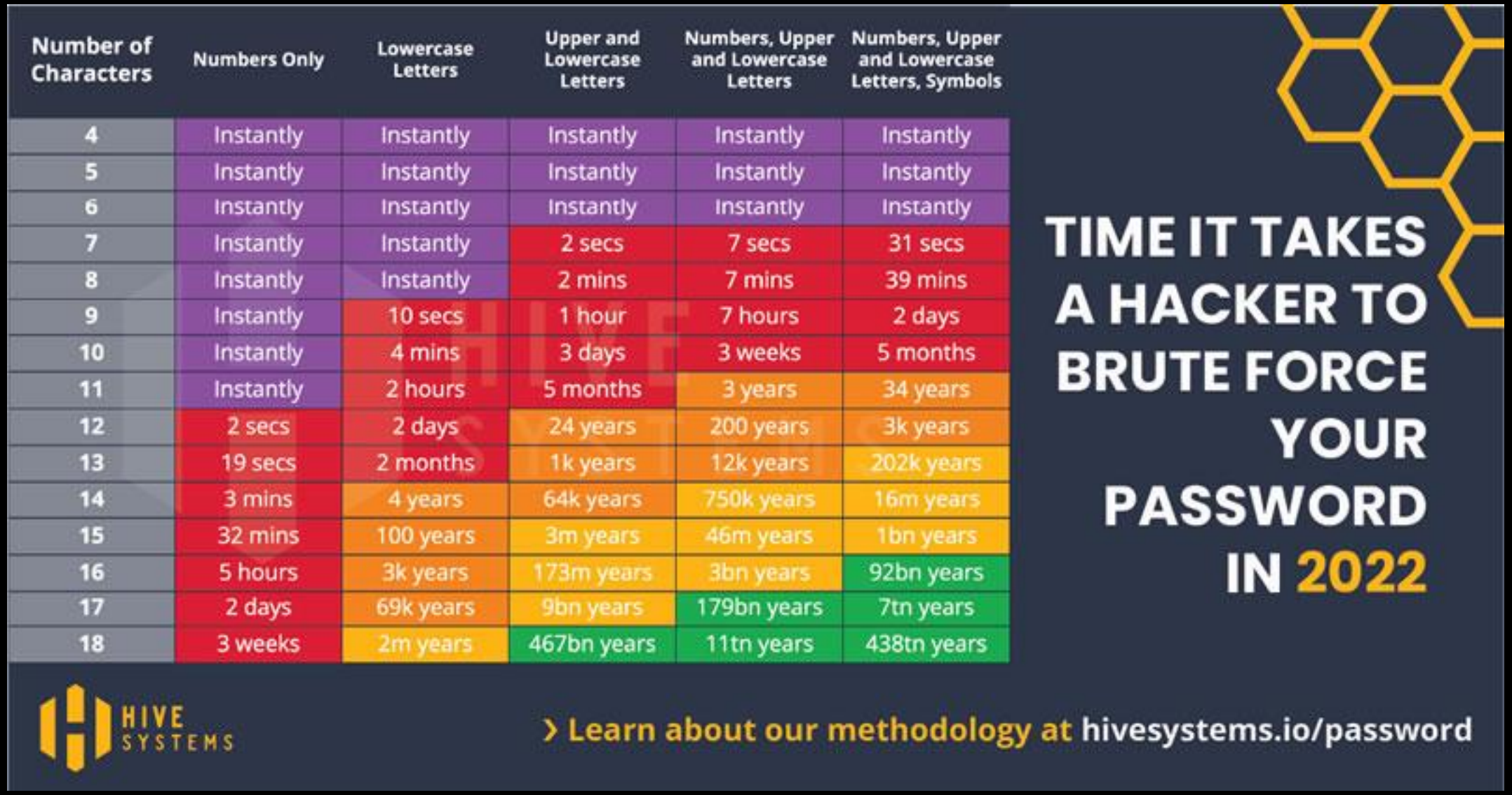
College of Nursing TRC

Topics

- Password Best Practices
- Identifying Fake Websites and Phishing Emails
- Travel
- Email
- File Storage Policies
- Questions

Passwords




Number of Characters
Numbers Only
Lowercase Letters
Upper and Lowercase Letters
Numbers, Upper and Lowercase Letters
Numbers, Upper and Lowercase Letters, Symbols
4 Instantly Instantly Instantly Instantly Instantly
5 Instantly Instantly Instantly Instantly Instantly
6 Instantly Instantly Instantly Instantly Instantly
7 Instantly Instantly 2 secs 7 secs 31 secs
8 Instantly Instantly 2 mins 7 mins 39 mins
9 Instantly 10 secs 1 hour 7 hours 2 days
10 Instantly 4 mins 3 days 3 weeks 5 months
11 Instantly 2 hours 5 months 3 years 34 years
12 2 secs 2 days 24 years 200 years 3k years
13 19 secs 2 months 1k years 12k years 202k years
14 3 mins 4 years 64k years 750k years 16m years
15 32 mins 100 years 3m years 46m years 1bn years
16 5 hours 3k years 173m years 3bn years 92bn years
17 2 days 69k years 9bn years 179bn years 7tn years
18 3 weeks 2m years 467bn years 11tn years 438tn years
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022
HIVE SYSTEMS
› Learn about our methodology at hivesystems.io/password

Password Best Practices

- Ensure a strong, unique password is set for all accounts
- Use a combination of upper- and lower-case letters, numbers, and symbols in passwords
- Use easy to remember passphrases rather than passwords, that have a minimum of 14 characters
- Never reuse passwords on multiple accounts
- Don’t use information in passwords that can be found in social media profiles (DOB, spouse or pet name etc.) or is known to others
- Ensure 2-factor authentication is set up, especially for accounts containing sensitive data
- Use a secure password generator to generate random strings of characters
- Avoid using dictionary words and commonly used passwords
- Use a password manager for creating strong passwords and secure storage, and set a long and complex passphrase for your password vault.

Email Security

7 Ways to Spot Phishing Email

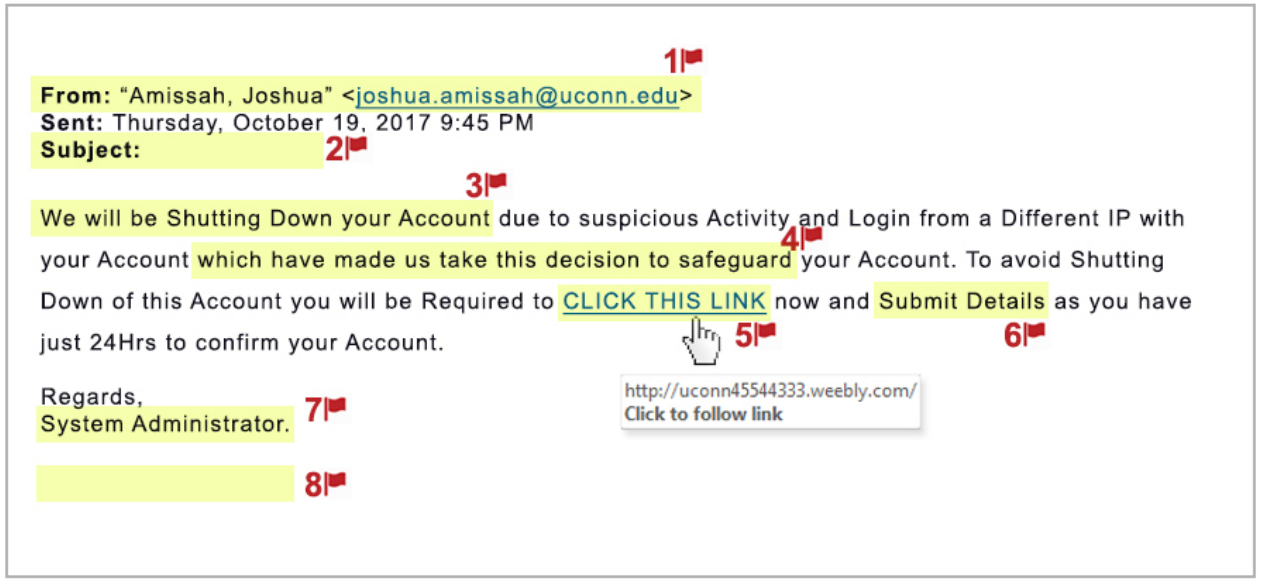
1. Emails demanding urgent action
2. Emails with bad grammar and spelling mistakes
3. Emails with an unfamiliar greeting or salutation
4. Inconsistencies in email addresses, links, and domain names
5. Suspicious attachments
6. Emails requesting login credentials, payment information, or sensitive data
7. Too Good to Be True Emails and Gift Card Scams

Emails demanding urgent action

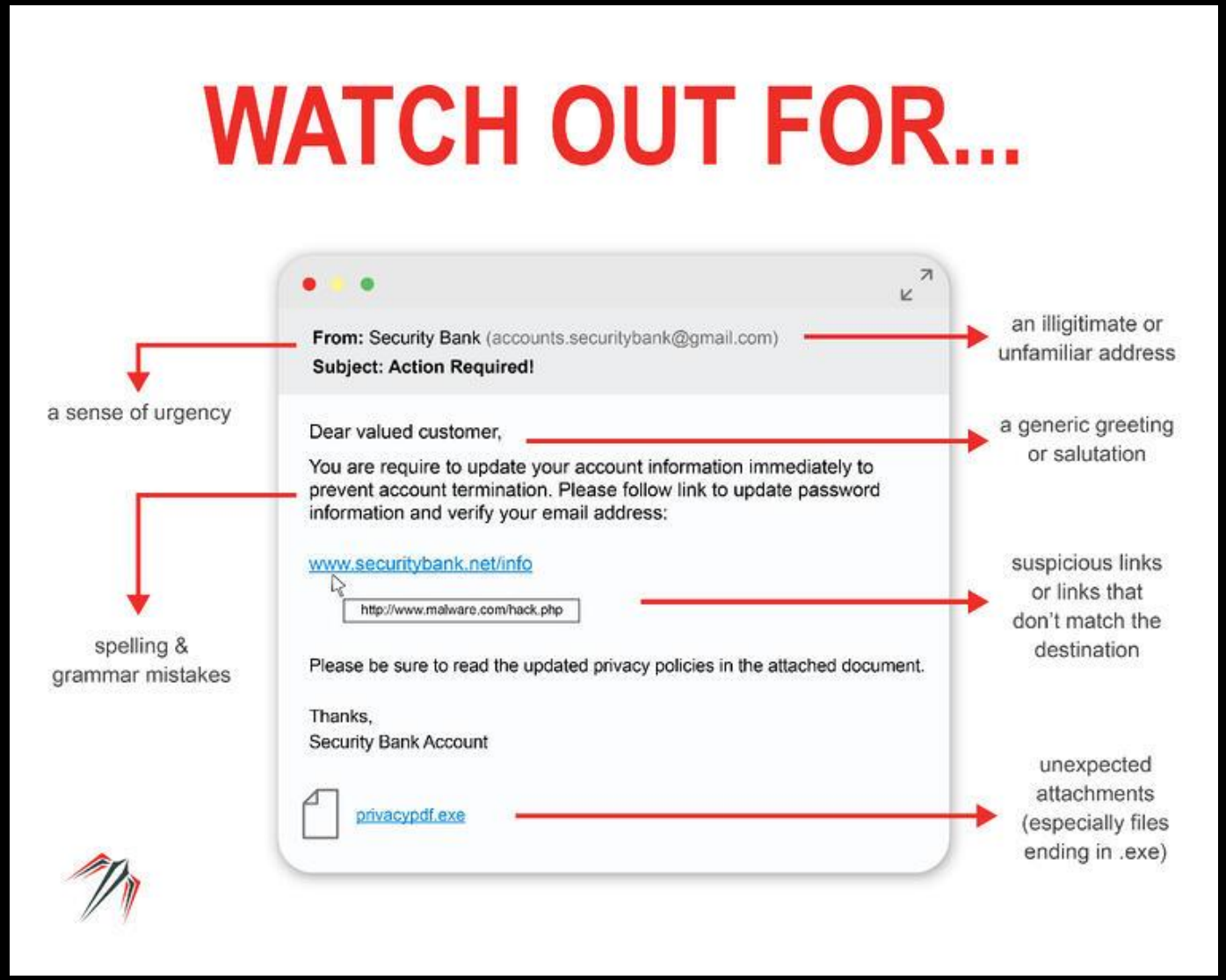
- Emails threatening a negative consequence, or a loss of opportunity unless urgent action is taken, are often phishing emails. Attackers often use this approach to rush recipients into action before they have had the opportunity to study the email for potential flaws or inconsistencies.
- Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often, they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams. They do that so that you won't think about it too much or consult with a trusted advisor who may warn you.
- **Tip: Whenever you see a message calling for immediate action take a moment, pause, and look carefully at the message. Are you sure it's real? Slow down and be safe.**

Emails with bad grammar and spelling mistakes

Below is a phishing message that targeted the UConn community. It triggers many red flags that identify it as a phishing message.



1. Even though this message comes from a UConn address, be wary. These can be easily spoofed or sent from a compromised account.
2. An official message from a University unit will have a subject.
3. The message uses urgent language to prompt a quick response.
4. This sentence is awkward and grammatically incorrect.
5. When you hover over this link, it displays a non-UConn address.
6. This message was an unsolicited request for personal information.
7. The signature line is generic. An official message would be signed by a person whose position and name you could verify.
8. There is no contact information. An official message would list UConn-specific contact information.



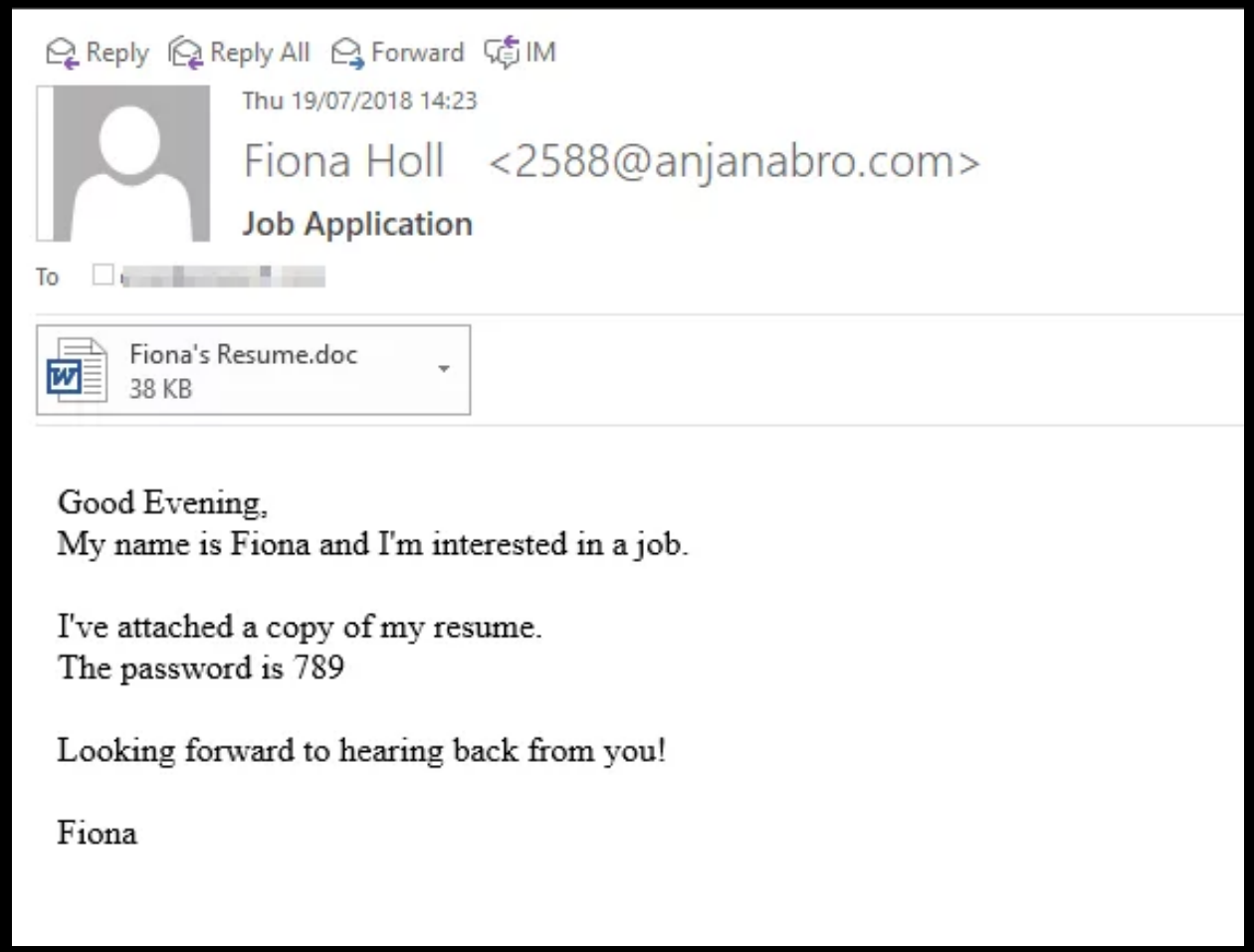
Emails with an unfamiliar greeting or salutation

An organization that works with you should know your name and these days it's easy to personalize an email. If the email starts with a generic "Dear sir or madam“, “Dear Lastname, First Name”, or even calls you by someone else’s name, that's a warning sign that it might not really be your bank or shopping site.

Inconsistencies in email addresses, links, and domain names

- Another way how to spot phishing is by finding inconsistencies in email addresses, links and domain names. Does the email originate from an organization corresponded with often? If so, check the sender's address against previous emails from the same organization. Look to see if a link is legitimate by hovering the mouse pointer over the link to see what pops up

- If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. Like microsoft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers.



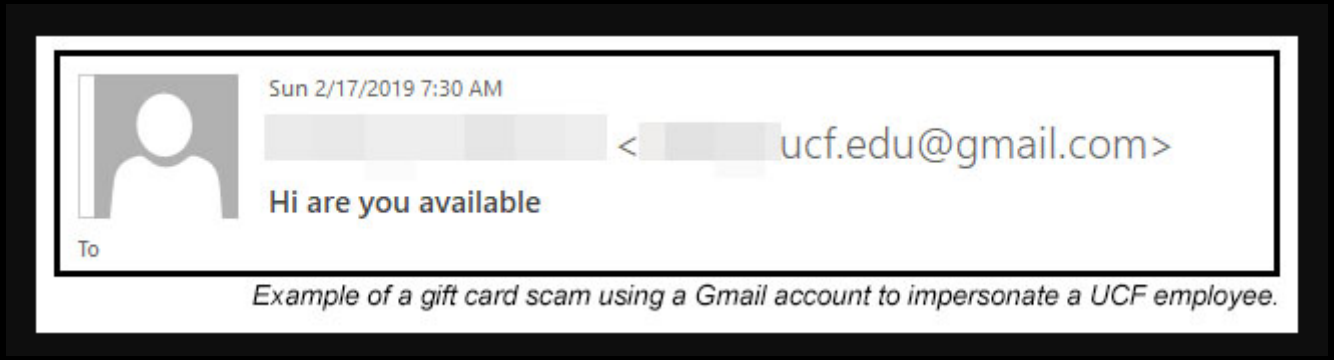
Emails with Suspicious Attachments

- Most work-related file sharing now takes place via collaboration tools such as SharePoint, OneDrive or Dropbox. Therefore, internal emails with attachments should always be treated suspiciously – especially if they have an unfamiliar extension or one commonly associated with malware (.zip, .exe, .scr, etc.).
- **Don't open any attachments you weren't expecting:** Like clicking on a link, once you agree to open an attachment, you open the door to possible harm.

Emails requesting login credentials, payment information, or sensitive data

- Emails originating from an unexpected or unfamiliar sender that request login credentials, payment information or other sensitive data should always be treated with caution.
- Spear phishers can forge login pages to look similar to the real thing and send an email containing a link that directs the recipient to the fake page. Whenever a recipient is redirected to a login page, or told a payment is due, they should refrain from inputting information unless they are 100% certain the email is legitimate.
- **DOIT AND THE UNIVERSITY OF SOUTH CAROLINA ARE NEVER, EVER GOING TO ASK YOU TO VERIFY YOUR CREDENTIALS VIA EMAIL.**
- **Never provide personal information: This includes your user ID, password, bank account information, Social Security Number, etc.**

Too Good to Be True/Gift Card Scams



Example of a gift card scam using a Gmail account to impersonate a UCF employee.

- Too good to be true emails are those which incentivize the recipient to click on a link or open an attachment by claiming there will be a reward of some nature. If the sender of the email is unfamiliar or the recipient did not initiate the contact, the likelihood is this is a phishing email. Amazon and Walmart are not going to give you a $500 gift card out of the blue.
- The initial email may start out innocuously, asking if you are available, stating that they need a favor, or asking for your phone number so you can receive text messages. Once you respond, the scammer will ask you to purchase gift cards, specifying the quantity and denomination. The message will ask you to scratch off the cards to reveal the codes, take pictures of those codes, and then reply back with those pictures.
- If you reply with the cards' codes, your money is now in the hands of the scammer. Gift cards are treated as cash, and in many cases, cannot be refunded.

If you receive a Phishing email

- Never click any links or attachments in suspicious emails. If you receive a suspicious message from an organization and worry the message could be legitimate, go to your web browser and open a new tab. Then go to the organization's website from your own saved favorite, or via a web search. Or call the organization using a phone number listed on the back of a membership card, printed on a bill or statement, or that you find on the organization's official website.
    - If the suspicious message appears to come from a person you know, contact that person via some other means such as text message or phone call to confirm it.
    - Report the message (see below).
    - Delete it.

How to report a phishing scam

- Microsoft Office Outlook - With the suspicious message selected, choose Report message from the ribbon, and then select Phishing. This is the fastest way to report it and remove the message from your Inbox, and it will help us improve our filters so that you see fewer of these messages in the future. For more information see Use the Report Message add-in.

- Outlook.com - Select the check box next to the suspicious message in your Outlook.com inbox. Select the arrow next to Junk, and then select Phishing.

Security for Domestic and International Travel

Security tips for Domestic and International Travel

- For members of the campus community, a trip to a foreign country presents unique data security challenges. The nature of international travel requires you to use your device (laptop, tablet or smartphone) in various unfamiliar places that may expose your data and device to malicious people and software.

- Staying digitally connected often means connecting devices to public networks in hotels, airports, train stations, and conference halls, which employ minimal security measures. Public networks can harbor malware from cybercriminals looking to steal your data for identity fraud, as well as nation-state actors targeting academic and business travelers(link is external) for intellectual property. In some cases, education networks are broadly targeted (link is external)by government agencies for the benefit of data theft.

- The next slide is a list of data security safeguards you should add to your travel checklist before, during, and after your trip. In addition to data security safeguards, international travelers also need to consider US export control laws and import restrictions imposed by the destination countries. If you have any questions about securing your data on your trip, please place a ticket with the Nursing Helpdesk.

Before you leave

- In the weeks before your scheduled travel date, please include the following data security safeguards to your travel planning routines
- **Leave your data and/or device at home.** The best way to safeguard your data or device is to not bring them on the trip. If you don't need to access data stored on your computer, leave your computer in a secure location at home and bring along a loaner computer instead. These can be checked out from the TRC.
- **Back up your data.** Whether you are traveling with a loaner computer, your regular computer, tablet, or smartphone, you should always back up your data. That way if you lose your data along with your device or malware corrupts it during the trip, you can be sure you have a good copy from which you can recover your data.
- **Use the CISCO VPN AnyConnect Software.** To protect against eavesdroppers on networks during your trip, install and configure VPN software to utilize full tunneling. Full tunnel VPN configuration will secure all internet traffic, whereas the alternate configuration, split tunneling, only protects internet traffic for USC internet services.

On the Road

- **Do NOT leave your device unattended**. Physically having control of your device is the easiest way for someone to access your data. Do not leave your device unattended in public, lend it to someone you just met or leave it in your checked bag on your flight. If you ever leave your computer, make sure to turn it off instead of just hibernating it or putting it to sleep.

- **Do NOT plug in untrusted accessories.** Untrusted accessories, those that came from questionable sources, can be infected with malware intended to steal your data. Avoid plugging in any untrusted accessories (flash drive, charging cable, SD cards, etc.) to your device. Try to plan and take all the necessary accessories with you, but if you must purchase an accessory abroad, make sure it is from a reputable source.

- **Do NOT enter your credentials into public computers.** Public computers such as hotel business center workstations and internet cafe computers are often poorly managed and provide minimal security protection for its users. If the need to use public computers arises during your travel, avoid entering your credentials at these public computers.

- **Connect only to known wifi networks.** It's tempting to stay in touch with friends and colleagues as you travel by connecting to wifi networks. However, anyone can create a network and give the network a legitimate sounding name, hoping to lure unsuspecting travelers to connect while capturing personal information transmitted through the network. This is especially prevalent at public cafes, hotel lobbies and airports. When connecting to a network, find out the correct network name from the staff at the business and connect to it.

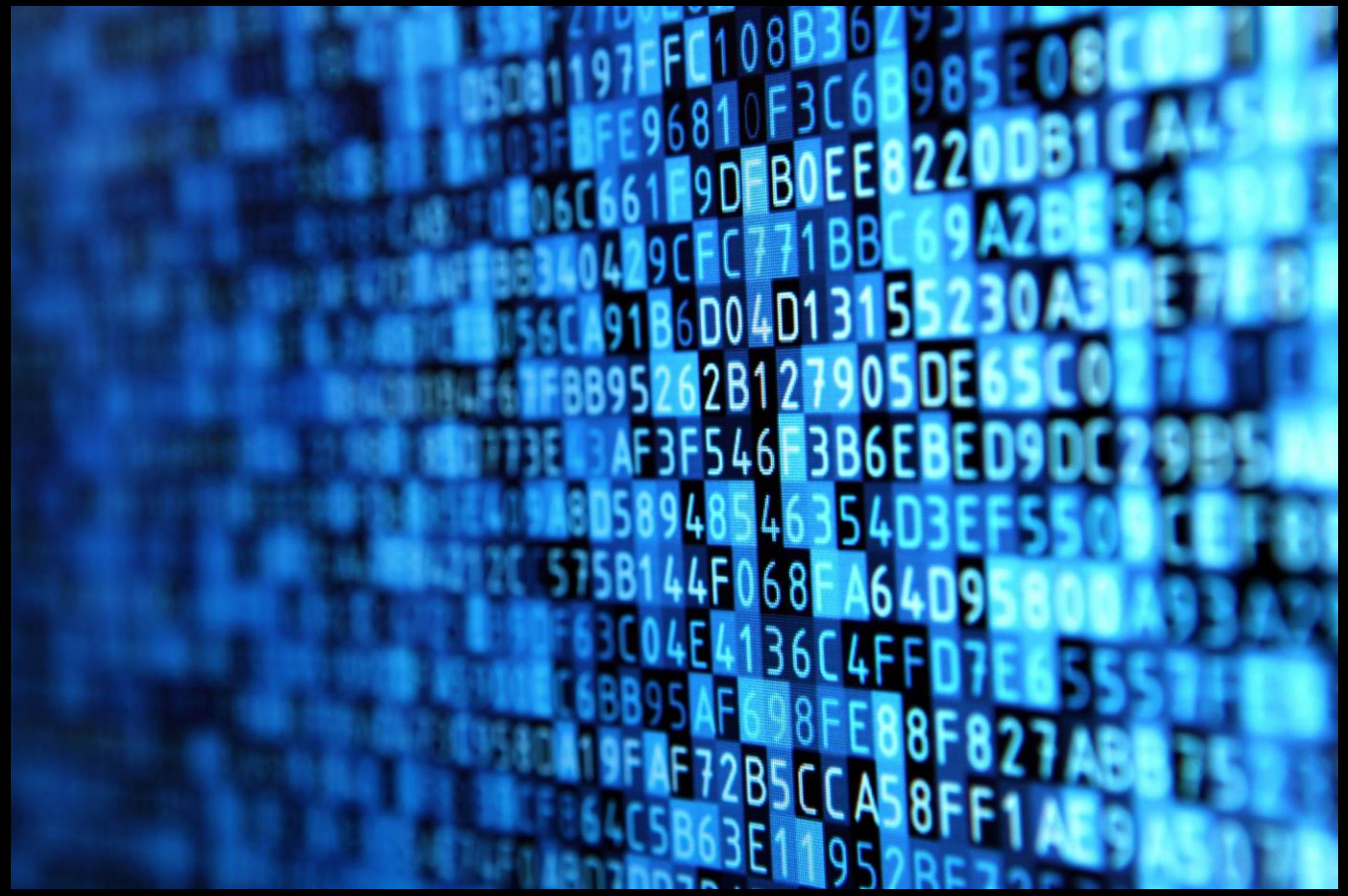
On the Road

- **Turn off your wifi when not in use.** Attackers can easily spoof Wifi network names to connect to devices within range for eavesdropping. To help you avoid accidentally connecting your device to rogue wifi networks at a later time, once you are finished using the network, turn off wifi on your device.

- **Use VPN Software to establish a secure network connection**. Not only does the VPN software provide access to USC services such as library services, it also creates a secure connection to USC that will prevent network eavesdroppers from gleaning private information when you use the network on the road. To take full advantage of the security provided by VPN software, be sure to utilize full tunnel configuration as noted above.

- **Practice safe web browsing.** The websites you visit online hold valuable data about you. They are also becoming gateways thru which hackers can steal your data by infecting reputable or seemingly reputable websites with malware. This threat is magnified during foreign travel as you connect to public networks in hotels, airports, cafes, etc at your destination.

Email Encryption



How to Encrypt Email

- Any email that has sensitive data must be encrypted. Encryption ensures that protected or sensitive information remain private during email transmission. This protects the individual and the university from potentially costly and reputation-damaging data breaches.

- **Types of email message that need encryption**

  Protected health information [PHI] (i.e., patient record information, etc.)
  Personally Identifiable Information [PII] (i.e., Social Security Number, specific identity information, etc.)
  Credit card information
  Any information protected by governmental or institutional regulations

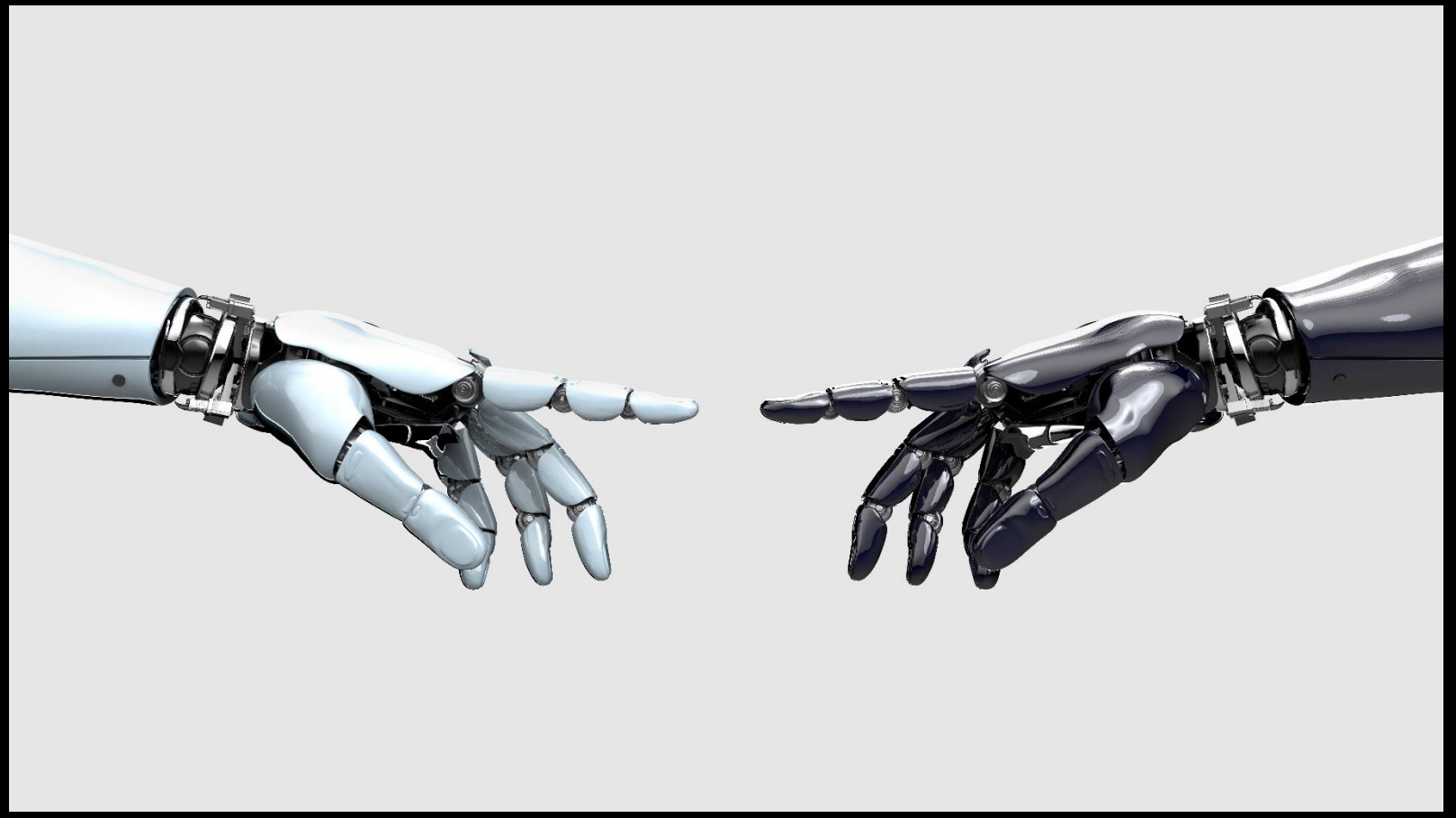
- **How to encrypt an email message**

  To send an encrypted message, use the encryption trigger **encrypt with brackets** (see options below) in the Subject line of the email message and send the message normally.

  <encrypt>, (encrypt), [encrypt], or {encrypt}

> The encryption trigger is not case sensitive <

Policies



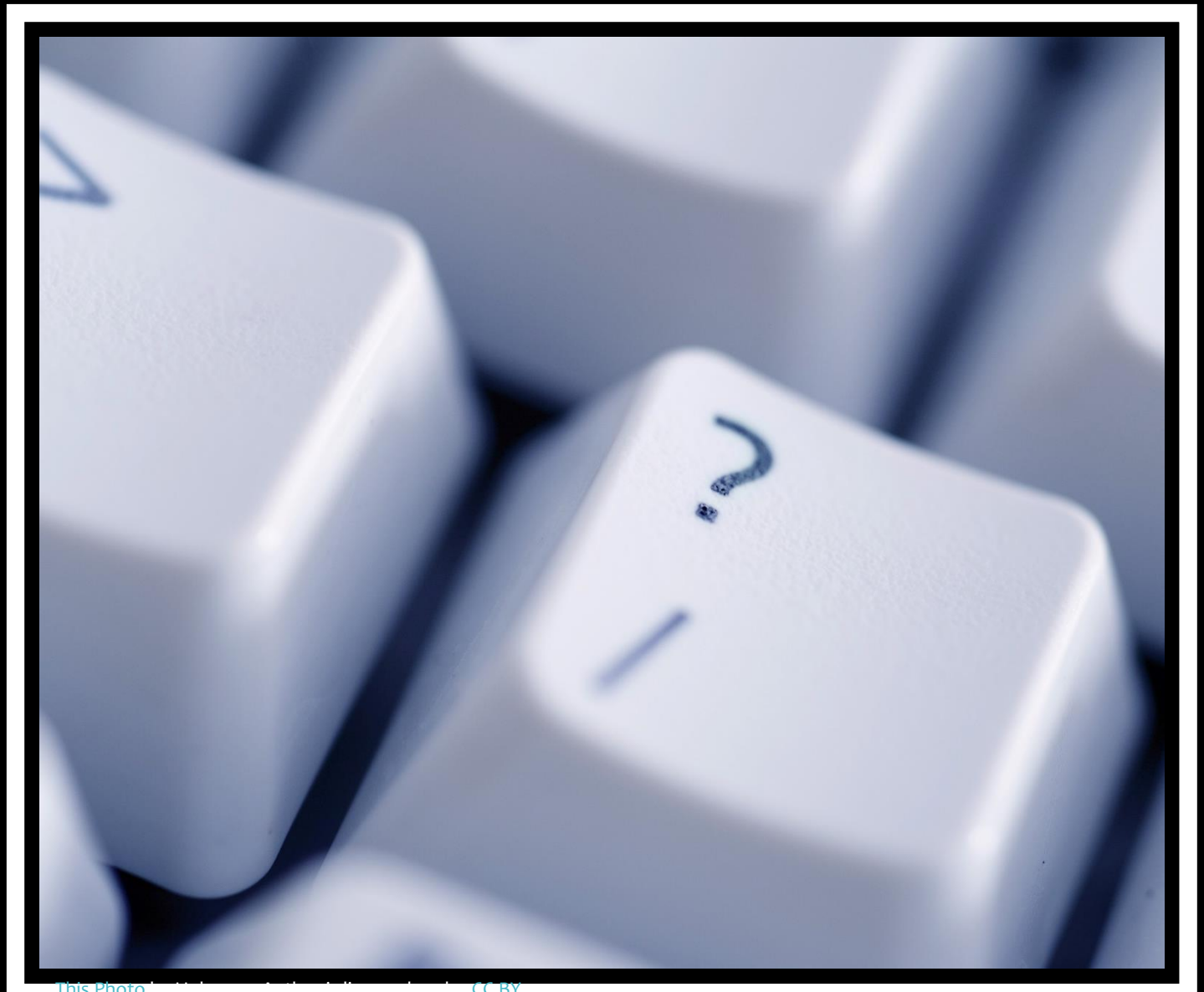
USC E-Mail Usage Policy

- **USC Email is subject to Freedom of Information Act (FOIA) requests.**
- **Employees and organization units must use university-provided email accounts for the conduct of University Business.** The email address should be one with a domain listed in Enterprise Data Standard 1.03, Email Domain Standard & Catalog.
- **Employees are prohibited from using personal or other external email accounts for University Business.**
- **Employee and organization unit email accounts must not be auto-forwarded to personal or other external email accounts;** this prohibits practices known as store-and-forward as well as forward-and- delete.

- This provision also applies to student employees when receiving and sending University Business-related email and organization units must use university-provided email accounts with a domain listed in Enterprise Data Standard 1.03, Email Domain Standard & Catalog and are prohibited from using personal or other external email accounts, for the conduct of University Business accounts. This provision applies to student employees when receiving and sending University Business-related email.

File Storage Policies

- The University of South Carolina provides Microsoft OneDrive cloud storage for all students, faculty and staff.
- EPHI and protected data should not be stored in OneDrive. Please contact the Nursing Helpdesk for storage options we provide.
- Alternatively, the primary investigators can set up a Microsoft TEAM account for their research group members to store images and data generated. Please place a ticket with the Nursing Helpdesk and we will start the process.
- Restricted data is NOT to be stored on the K: drive.
- Files are subject to State of South Carolina file retention policy.



This Photo by Unknown Author is licensed under CC BY

Thank you!

Questions?