Top 10 Actions to Reduce Risk [1]

All members of the CU community are responsible for ensuring necessary protections are in place to keep our sensitive information secure, whether working from the office or working remotely. Reduce the risk of an incident or breach by incorporating the following security-positive behaviors into your computing routine.

1. Use safeguards when working remotely.

When working from home or another remote location, your responsibility for protecting sensitive university information remains unchanged.

Use these safeguards to avoid unauthorized or accidental access, use, modification, destruction, or disclosure of sensitive university information:

- Only university-provided computers, including mobile computing devices, should be used to access or handle sensitive university information. If you must use a personal computer, it is recommended that you use remote desktop to connect to your university-provided computer.
- Secure your home Wi-Fi router by using a strong, unique password, and make sure encryption is enabled.
- Boost Wi-Fi security with a virtual private network (VPN) at home and when traveling; it provides a secure connection to the CU network from any location and may be required to access many CU-specific drives and applications. Be sure to connect to the VPN *before* using unsecured networks or public Wi-Fi.
- Do not allow other household members to access your university-provided computer. Unauthorized individuals may unknowingly put your computer at risk. Always lock your computer when stepping away from it, just as you would in the office.
- When scheduling virtual meetings, consider using passwords or waiting rooms to control access. (Do not share meeting details, such as links and IDs, on public forums.)
- Be mindful when sharing or discussing sensitive university information in virtual meetings. Only share such information with the people who need to know it for an authorized use. This includes verbal and written information.
- Protect paper documents containing sensitive university information.
  - When not actively being worked on, lock the paper documents behind two layers of protection: a lockable file cabinet or storage container (with the key location or passcode unknown by household members) and the locked room or house where the cabinet or container is stored.
  - If you do not have the ability to keep the paper documents locked away, consult with your department about providing a locking cabinet or container for the duration of the work.
  - Dispose of the paper documents using a crosscut shredder or keep them locked

away until you return to your campus office.

Visit your IT department's website for campus-specific information [2] on VPN, encryption, remote desktop, and collaboration tools.

International travel – know before you go

High-risk foreign counties are often governed by laws that restrict how you conduct university business. If you are traveling internationally, be familiar with laws and policies pertaining to technology and take the appropriate precautions to secure your university-provided device if it contains controlled software or sensitive university information or both.

Visit the Institutional Statement of Export Control Commitment and Support [3]website for more information about your campus office contact, policies, and guidance.

2. Report a potential incident.

If you believe an information security incident has occurred, it is important to report it as soon as possible. This allows the investigative team to act quickly to determine the level of impact and contain the incident.

Visit Reporting an Incident [4] for more information.

3. Recognize phishing, other deceptive tactics.

Cybercriminals use deceptive tactics to manipulate people into doing what they want with the goal of stealing information and money. The tactics, sometimes called “social engineering,” are the foundation of all phish and scams conducted through emails, text messages, phone calls, and in-person interaction.

Here are some things to remember:

- Do not provide your username, password, or any personal information requested by unsolicited email or phone call. (CU will never ask you for your password.)
- Be wary of email links or attachments, unless you are positive the content is safe.
- Don't react to tactics aimed to scare you into taking urgent action, including: threats of a lawsuit, a computer full of viruses, locked accounts, or opportunities to earn or save money now.
- Legitimate companies and service providers will provide a way for you to contact them directly. If you’re uncertain, you can learn more by researching them online.
- Emails from a university leader asking you to make a urgent wire transfer or buy gift cards are likely to be scams.
- No one from your campus IT department is going to call to inform you about a computer virus and ask for your passwords.
- Government agencies will not call and threaten you, or make demands for payment in the form of gift cards.

Visit Phishing Scams FAQs [5] for more information.

4. Protect sensitive university information.

If you access, handle, or store sensitive university information, you are responsible for safeguarding it from unauthorized or accidental access, use, modification, destruction, or disclosure.

The information, classified as “Highly Confidential” and “Confidential,” is only for the “eyes of the authorized individuals” in any form including paper or electronic.

Be able to recognize sensitive university information. Some examples include:

- Protected health information
- Social security numbers
- Payment card numbers
- Health insurance policy ID numbers
- Student information and admission applications
- Faculty and staff personnel records, benefits, salaries, ID numbers, and employment applications
- Donor contact information and non-public gift amounts
- Non-public policies
- Internal memos and email, and non-public reports
- Purchase requisitions, cash records, budgetary plans

Take these actions when accessing, handling, or storing sensitive university information:

- Only share with the people who need to know it for an authorized use. This includes verbal and written information.
- Encrypt the information when transmitting or storing.
- Ensure networks or systems used to handle or store the information has appropriate firewalls, monitoring, logging, patching, anti-malware and related security controls.
- Use university-provided computers, including mobile computing devices and storage medium.
    - If this is not possible and you must use a personal computer, for example when working remotely, use remote desktop to connect to your university-provided computer.
    - Additionally, please do not allow other household members to access your university-provided computer. Unauthorized users may unknowingly put your computer at risk.
- Refer to the universitywide policy [6] for information retention and disposal.

Visit the Data Classification [7] webpage for more information.

5. Keep devices secure.

- Back up files regularly.
    - This is invaluable if the device is lost, stolen, or compromised and needs to be wiped clean.
- Boost Wi-Fi security with VPN.
    - Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your laptop or smartphone while you are connected to them. Using a virtual private network (VPN) provides an added

    - layer of security by encrypting internet traffic. Be sure to connect to the VPN *before* using unsecured networks or public Wi-Fi.
- Keep software, including antivirus, updated.
- Keep tabs on your applications.
    - Your mobile device may contain suspicious apps running in the background, or using default permissions you never realized you approved—gathering your personal information without your knowledge. Check your app permissions and delete what you don’t need or no longer use.
- Enable encryption to keep files and folders unreadable to unauthorized people.
    - This is especially valuable if your device is lost, stolen or compromised.
- Avoid using public charging stations by having a phone backup battery.
    - Criminals set up fake charging stations that allow them access to your device.
    - If you must use the charger, use a USB data blocker.

Visit your IT department's website for campus-specific information [2] on VPN, antivirus, and encryption.

6. Create strong, unique passwords.

Weak and reused passwords make it easier for cybercriminals to gain access to your computing devices, applications, files, and accounts.

Use these tips to create strong passwords and keep them private:

- Go beyond the minimum requirements set by your campus if you can. The US Department of Defense requires a minimum of 15 characters in a password, which is a good rule to follow.
- You can make a password that appears random by making up a passphrase that means something to you, and only using the first letter of each word. For example, the phrase “My first job in 94 was delivering pizzas!” could become the secure password “M1stji94wdP!” Or choose some numbers, letters, and symbols and invent a mnemonic based on what you chose.
- Don’t use the same password for multiple sites. If you use the same password, a single compromise of that password puts all your accounts at risk.
- Use two-factor or multifactor authentication whenever it’s available to help prevent unauthorized access to your devices and accounts (e.g., a unique one-time code sent to your phone or mobile device).
- Consider password managers to generate and remember different, complex passwords for each of your accounts.
- Keep your password to yourself, and don’t create opportunities for someone else to steal your information:
    - Don’t tell other people your password.
    - Don’t write your password down.
    - Don’t allow your browser to save your credentials or automatically fill your credentials for you. If you can log in automatically, so can anyone else with your device.

Visit your IT department's website for campus-specific guidance [2].

7. Be on the lookout for insider threat.

An insider threat is the threat that an employee or a contractor will use authorized access to compromise the confidentiality, integrity or availability of private or sensitive information.

Here are some possible warning signs of an insider threat:

- Working odd hours without authorization.
- Taking proprietary or other sensitive information home without need or authorization.
- Copying material unnecessarily, especially if it’s proprietary or classified.
- Installing personal software or hardware in violation of policies, accessing restricted websites, conducting unauthorized searches, or downloading sensitive material.
- Taking short trips to foreign countries for unexplained reasons.

If you see suspicious behavior, report it to your campus IT or information security department [8].

8. Only use CU-approved applications.

Avoid the possibility of malicious software by only using applications that are approved and supported by the university. Consult with your campus IT department [2] before acquiring new applications.

9. Protect the privacy of those in CU community.

Your job function may require that you handle private information related to students, employees, alumni, donors, research sponsors, patients, and others. (Examples of such information includes social security numbers, credit card information, educational records, and health information)

Consider these actions when handling private information:

- Ensure there is a true business need for collecting personal information.
- Only request the minimum information required. Resist the temptation to collect additional information that you “might” need in the future.
- Inform the individual why you need the information and what it will be used for. If the information will be handled by a third-party, clearly disclose that, too.
- Follow CU security standards and consult with the information security office to properly secure personal information. Most notably, limit access to personal information to only those who need to know.
- Have a data retention plan that includes a schedule to delete personal information when it is no longer needed. Have a plan for deleting old information and have processes that ensure information is cleaned up according to that plan.
- Be aware of any regulatory or contractual requirements regarding privacy and security. Be sure you know your obligations and come up with processes to meet them.This may mean meeting specific security standards, minimum/maximum data retention requirements or other required steps.
- Know how you will handle privacy related questions and requests. Privacy@cu.edu [9] can assist or connect you with others at CU to help with privacy concern

10. Trust your instinct.

If something seems suspicious, it probably is. We rely on you to identify and report events that are not routine. You don't have to be an expert. Contact your campus IT or information security department [2] to look into it for you.

Groups audience:

Office of Information Security

Source URL:https://www.cu.edu/security/awareness/top-10-actions-reduce-risk

Links

[1] https://www.cu.edu/security/awareness/top-10-actions-reduce-risk [2] https://www.cu.edu/security/about [3] https://www.cu.edu/export-control
[4] https://www.cu.edu/security/reporting-incident [5] https://www.cu.edu/security/awareness/phishing-scams-faqs [6] https://www.cu.edu/ope/aps/2006 [7] https://www.cu.edu/ois/data-classifications-impact
[8] https://cu.edu/security/about [9] mailto:Privacy@cu.edu