SecureCat Courier is UA’s monthly cybersecurity newsletter, distributed by Information Security Liaisons to UA faculty and staff.

No, it’s not exciting, but understanding what goes into handling data securely not only makes life easier for you; it protects critical University information assets, such as:

- Credit card numbers
- Research findings
- Student grades and records
- Employee personal information
- Protected health information

This month’s issue provides useful information on handling data, whether it be electronic or in hard copy form, especially your own and the University’s sensitive data.
Data Sec-U-R-IT-y. . . you are IT!

While it is cliché to say that data is worth more than gold, it is verifiably accurate. You can lose a lot more than just money if someone has your Social Security number and birth date. Password compromises can lead to re-routed paychecks and drained bank accounts.

Here are tips for keeping your data secure:

1. **View all emails with skepticism.** Don’t open attachments from an unknown source, reply with sensitive information included in the reply, or click on links to unknown websites.

2. **When shopping online, be careful about where you enter sensitive information.** Look for “https” and a lock icon on the bottom of webpages. Also, if an offer seems to be too good to be true, it is.

3. **Protect your mobile devices.** Our cell phones and tablets carry information that, if in the wrong hands, can turn your life upside down. Use passcodes and thumb prints to lock your devices, install secure-wipe software, and keep track of your phone the way you do your wallet and credit cards.

4. **Use encryption.** If you can encrypt your computer, tablet, and phone, do so. That way, your information will be secure, even if your device is lost or stolen.

5. **Connect securely to the internet.** If you are on a wireless connection, make sure it’s a secure connection (password-protected). If you have to use unsecured wifi, use the University’s VPN (virtual private network) to protect your data.

6. **Be aware of your surroundings.** Physical security is essential to data security. Lock up your valuables when they are not with you. Shred paper containing sensitive information when disposing of it. Be cautious in empty parking lots and other unsecured physical locations.

For more tips on securing data, visit our [website](#).

---

**Data Security at UA**

UA Information Security provides a variety of resources on our website to assist UA employees in understanding how to secure the University’s information assets. Here is a sampling of the information you will find on our [Data Management webpage](#):

- **Office Security @ UA**
- **Should I Retain or Dispose of This Document?** This flowchart will help you in determining what you should keep or toss (either electronically or in hard copy)
- **Safeguarding Computer Equipment during Office Moves and Renovations**

---

**UA’s Data Classification and Handling Standard**

In information security, it’s all about the data. UA’s Data Classification and Handling Standard provides detailed information on how data should be protected, especially data controlled by regulatory requirements. Visit our [website](#) to view classifications and handling requirements.
Faculty Sensitive Data Checklist

In the course of teaching over many years, data are moved from one device to another so that faculty can respond to their former students’ requests for references. While this is convenient, it can lead to data leaks. This easy checklist will help you in gaining hard drive space, as well as protecting your former students’ data from unintentional exposure.

Please take a few minutes to check on your risk:

☐ Did you teach classes in 2008 or prior years AND did you keep an electronic class roster on your computer with student names and grades? If so, it is very likely that the rosters are in Excel files, contain student names and IDs and that the IDs contain social security numbers. UA was in the process of remediating SSNs, but had not completed all students.

☐ Look in directories/folders of classes that you teach for semesters/years in 2008 or earlier and for Excel or other files storing class roster data.

☐ Do you conduct research that involves details about individuals AND does the data include demographic data including SSN, Driver’s license, family names, addresses, phone numbers, etc.? You may need to check your data repositories to be sure about some of these elements. Often research involves a specific situation that may cause embarrassment to study participants.

☐ Look for research data containing personal information about student participants or research under compliance regulations from national agencies (these data should be encrypted).

Remediation Options:

- Deleting the file is the best course of action if enough time has passed that the final grade on record is all you would need for any inquiry.
- Alternatively, delete all student IDs and resave the file.
- Encrypt the data if you feel you must keep it.

Please contact your local IT support or UA Information Security at 621-8476 for more information.

All-Employee Security Awareness Training now available in UAccess Learning!

Visit [UAccess Learning](#) to enroll and complete this valuable training!

Would you like to promote security awareness in your department? Download our custom screensavers!