Security Guidelines

Last Modified on 11/22/2023 1:45 pm EST

Security is a responsibility shared with you, Wharton Computing, and the Wharton Information Security Office. Working together, we can ensure that your data and the School remain secure. This article provides guidelines and best practices that you can use in your day-to-day activities to enhance and maintain the security of your University-related accounts and information.

> If you have any questions or concerns about anything in this article, please reach out to the Wharton Information Security Office at security@wharton.upenn.edu.

The Wharton Computing Accounts & System Policies article contains more information about specific account and system policies.

Security Best Practices

The following best practices apply to all Wharton faculty, staff, and students. We are all part of keeping our data and colleagues protected.

Share Safely

Information containing private or sensitive data ("High" and "Moderate" data according to the Penn Data Risk Classification) may only be shared or accessed in accordance with the University's Information Security Policy.

Secure sharing options include:

- Wharton-approved cloud storage accounts (PennBox, Dropbox)
- SecureShare

> Always take a moment before you share any data to think about what data is included and if it is considered private by the University or your department.

Protect Information & Systems

Protecting data is important; to do that, the data must be stored in a secure and appropriate place. Protect all information on all systems. University data's confidentiality must be safeguarded, no matter where it resides.

As you think about the safeguards you have in place, remember:

- You have to know the risk to prevent it. Know the level of classification that your data falls into so you can make appropriate decisions regarding its protection.
- Your Wharton Computing Representative is always willing to talk with you about measures you can take to enhance protections.
- The Wharton Information Security Office is available to assess your data and make recommendations around storage and necessary protections.

Report Possible Problems

Security incidents happen; the sooner we know, the sooner we can help.

Report any unauthorized access or suspicious behavior related to Wharton's confidential data or system as soon as possible. If you suspect Wharton's information has been exposed, please contact Wharton's Information Security Office.

Ways You Can Help

The best way you can help the Penn community is to be familiar with University Information Security and Privacy policies. In addition, practicing the following will help keep everyone secure:

Manage your Password

A strong and unique password is essential to account security, as your password is the front line and often the only defense against someone with malicious intent. The strongest password is unique, random, and at least 15 characters.

At a minimum, we recommend a password containing letters, numbers, and symbols and using unique passwords for all your websites/services. Our article about password guidelines and tips is written to cover PennKey and Wharton account passwords specifically but can be applied to any other account.

The elements of a good password also, by nature, make those passwords difficult to remember. Add in the fact that you should be using different passwords for each service you encounter, and suddenly, you have a large number of difficult-to-remember passwords you need to remember!

To help with this, **Wharton offers premium access** to a service called LastPass. This is an *encrypted password manager* that stores your account credentials for you. You will only need to remember the Master Password for your LastPass account, which then stores all your other passwords. This will allow you to create & set very strong passwords while not having to remember all of them.

To learn how to access this service, see our LastPass: Managing Passwords (and more) at Penn article.

Antivirus

Wharton Computing offers free virus protection software for both Windows and Mac users to help keep your devices safe from viruses and spyware. To learn more about this service, see our Antivirus article.

> For staff & faculty, your Wharton-owned and managed computers should already have antivirus installed on them.

Two-Step Authentication

Two-step authentication provides an additional layer of protection when accessing your account(s), and we recommend you enable it for any accounts that support it. For more information about two-step at Penn, see our Two-Step Verification starter article.

Phishing

Phishing messages are crafted to appear legitimate, but they are designed to trick you into sharing data or access

with hackers.

If there is the least hint that a message may not be what it seems, take the time to verify it or contact yourWharton Computing representative to confirm. We would much rather help you determine a message is not a threat than have you (and us) subjected to the consequences of a phished account.

To learn more about phishing, see our Phishing article.

If you think your account has been compromised, see our Compromised Account article to find out what to do.

Copyright/Student Conduct

Materials subject to copyright or license restrictions should not be openly shared on the PennNet network, nor should any related activities take place. Doing so may result in disciplinary sanctions and/or fines.

To learn more about the policies, see the Office of Student Conduct (OSC) website and File Sharing and the Penn Acceptable Use Policy on Electronic Resources.

Useful Resources

- Wharton Information Security Office
    - Email: security@wharton.upenn.edu
- University Information Security Policies
- University Data Risk Classification
- University Privacy Policy
- Partner with Wharton's Information Security Office : they can provide security & privacy guidance, security risk reviews/assessments, support, and more.

Questions?

Faculty & PhD Students: Academic Computing Services

Staff: Administrative Support

Students: Wharton Computing Student Support