IT Security Checklist

The following guidelines were developed to help users operate computers securely and to protect sensitive information. Please contact the IT Help Center at 303-871-4700 or in person in the Anderson Academic Commons if you have questions or need help implementing these guidelines. Additional contact information and resources are available at: http://www.du.edu/it/contact. If you would like to download a copy of the IT Security Checklist, please visit https://go.du.edu/ittips.

1. Never respond to email or phone calls requesting verification of username and/or password. If you receive a request for this type, please notify the IT Security Team at abuse@du.edu. Also, please report suspicious emails by clicking the "Report Phish" button in Outlook, so the team can investigate.

2. In the same manner do not respond to suspicious links in email messages or web pages. Doing so may allow malware and computer viruses to be downloaded to your system. Always look at the address bar of your browser to make sure you are at a site you are familiar with. It is important to know how to spot a fake website so you don't fall prey to a phishing scam.

3. Install CrowdStrike antivirus/antimalware software on your computer. This software is available in PioneerWeb (under the "Resources" tab) for Windows and Apple operating systems, and is available for use on DU owned machines as well as personal machines of faculty, students and staff.

4. Be sure to have software updates performed on all of your computer operating systems and applications. The links on the following page provide information for Microsoft and Apple products.

5. Use secure passwords that can't be easily guessed. And protect your passwords by not having them accessible. Guidelines for selecting secure passwords are given on the following page.

6. Use email encryption when sending sensitive information off campus. For information on doing this within Office 365, please see the link on the following page.

7. Use Eduroam instead of DU WiFi for wireless connectivity on campus. This offers a secure connection not only at DU but also at member universities and research centers.

8. Do not store sensitive information on unsecured flash drives or other devices. The IT Help Center can put you in touch with a security specialist who will advise you on secure encrypted methods of storing sensitive information.

9. Make backup copies of files or data that you are not willing to lose. The IT Help Center can advise you on options for data backup in both Windows and Apple environments.

10. Secure laptop computers and mobile devices at all times. Shut down, lock, log off, or put your computer and other devices to sleep before leaving them unattended. Most importantly make sure they require a secure password to start up or wake-up.

A few helpful links:

How to spot a fake website
http://www.dell.com/downloads/ca/support/spot_fake_website_not_get_phished_dell_en.pdf

Antivirus software available at DU
go.du.edu/antivirus

Maintaining software updates on your Windows and Apple computers

Microsoft: https://support.microsoft.com/en-us/kb/311047
Apple: https://support.apple.com/en-us/HT201541

Sending an encrypted email message
go.du.edu/encryptedemail

Eduroam at DU
go.du.edu/eduroam

Proofpoint Email Protection
https://www.du.edu/it/services/software/proofpoint

LastPass Password Manager
https://www.du.edu/it/services/software/password-management

DU IT Help Center information
The IT Help Center is housed in the Anderson Academic Commons located at 2150 E. Evans Ave. Please click here for a printable PDF map of campus building locations.

Phone Support: 303-871-4700

- Hours: Open 7 days a week. For hours, please visit http://www.du.edu/it/contact

Password Guidelines

Passwords (including pass phrases, PINs *etc*.) must be:

- Kept confidential and not shared (except for specifically authorized shared/group userIDs);
- Memorized or stored in a secure password storage system rather than written down;
- Easy to remember but hard to guess (*e.g*. no dictionary words, variants of University of Denver or the user's name, project or department names, locations, simple keyboard sequences *etc*.);
- At least eight characters long (ideally 12 or more characters for privileged userIDs);
- Composed of a mixture of characters, including mixed case letters, numbers and punctuation marks;
- Changed at the first opportunity by the users to whom they are initially issued and at least once every three months thereafter;
- Changed immediately if there is a significant possibility of system or password compromise (*e.g*. if someone who knows a shared password leaves the University, especially following any form of security incident);
- Different on different categories or types of system or userID (*e.g*. University of Denver and non-University of Denver systems, ordinary and business-critical systems, non-privileged and administrator accounts);
- Successive passwords must be substantially different, avoiding simple sequences;
- Passwords must not be included in any automated logon process, nor stored on disk without encryption for example in scripts, parameter files *etc*.