**1. What are my information security responsibilities?**

All members of the University community—students, faculty, and staff alike—are responsible for protecting the IT resources they use or manage. Access to the University's information, devices, and systems is a privilege, and everyone who has access has a duty to use it [**responsibly**](https://www1.udel.edu/security/bestpractices/acceptableuse.html) and in accordance with information security procedures and requirements.

**Bottom line: You are responsible for protecting the IT resources you use.**

**2. I have other job responsibilities. Will my security responsibilities prevent me from fulfilling them?**

Not at all. Security requirements aren't meant to distract you from your other responsibilities; they're meant to equip you to keep yourself, the University, and the community safe from cyber threats.

Information security is already a part of your workday. Each time you sign in to your computer or UDelNet account, you're practicing security. Many security requirements are exactly these kinds of small tasks; if they aren't already part of your daily routine, they will take you only moments to complete and will soon become second nature.

**3. How do I learn more? Is there training I can take?**

Faculty and staff can take [**Secure UD Training**](https://www1.udel.edu/security/training) to improve their awareness of information security issues. Secure UD Training is a modular, self-paced, online training program that helps employees identify and address threats and concerns regarding computing and information security. If you aren't already enrolled in training, contact the [**IT Support Center**](https://www.udel.edu/it/help/request) to request your enrollment.

All members of the University community can also use the resources available on this website to learn more about the University's [**new information security efforts**](https://www1.udel.edu/security/news), [**best practices for computer and information security**](https://www1.udel.edu/security/bestpractices), and the [**tools and services**](https://www1.udel.edu/security/resources) available to help protect you and the University.

**4. Why are strong passwords important and how do I create one?**

The strength of your password directly affects how easy it is to guess that password or how long it takes a hacker to crack it. In many cases, hackers gain access to an account because the account's owner set a weak password.

To set a strong password, follow [**University password guidelines**](https://www1.udel.edu/security/bestpractices/passwords.html):

* Create a longer password. The more characters you use, the harder the password will be to guess and the longer it would take to crack. UDelNet passwords must be between 12 and 30 characters long.
* Never use a single dictionary word or name as your password.
* Use a variety of characters, including uppercase letters, lowercase letters, numerals, and special characters like punctuation marks.
* Never choose an obvious password like "password," "password1," "12345," or "00000."

If you have a hard time remembering passwords containing random characters, try using a passphrase, which is a string of words used as a single password. For example, "ClevelandChapelLovettAcademy," or "**[CorrectHorseBatteryStaple](https://xkcd.com/936/" \t "_blank)**" are both passphrases with 25 or more characters, but they can be easier to remember than randomly generated passwords even 15 characters long!

**5. What is two-factor authentication (2FA)?**

[**Two-factor authentication (2FA)**](https://www1.udel.edu/security/bestpractices/2fa.html) is a means of protecting your digital accounts from unauthorized access and use.

Typically, you log in to an account by providing your username and [**password**](https://www1.udel.edu/security/bestpractices/passwords.html). This is a quick way to log in, but hackers can easily access your account if they steal or crack your password. However, if your account is protected by 2FA, then you will need to provide the standard username and password combination and then a second authentication factor (such as a temporary security code or the answer to a security question) to log in. Even if hackers steal or crack the password to a 2FA-protected account, they still can't log in to it without the second factor.

2FA is available for your UDelNet account, and you're strongly urged to [**sign up for 2FA**](http://www.udel.edu/it/help/2fa/) to help protect your account from theft and misuse. You're also urged to enable 2FA protection for your other sensitive accounts, such as your banking, credit card, tax filing, and investment accounts.

**6. What is phishing and how do I avoid it?**

[**Phishing**](https://www1.udel.edu/security/phishing/) is a cyber attack in which scammers send fake emails with intent to steal your personal information or get you to download malware. Common examples of phishing emails include unexpected "special offers," notifications that your email account is reaching its quota or may be suspended, or classic scams like the Nigerian advance fee fraud.

Most phishing emails use common tactics:

* A fake or spoofed sender to create a sense of legitimacy. For example, "IT Help Desk" or a name from your contact list.
* A sense of urgency. For example, "Your account will be deactivated in 24 hours."
* Typos, poor grammar, unusual wording, or other obvious errors.
* Links that don't go to real or legitimate websites. For example, "udel.com" or "udel.edu.biz."
* Suspicious attachments. For example, an unexpected "court summons" or "the files you asked for."

[**Spear phishing**](https://www1.udel.edu/security/phishing/be-aware.html#what-is-phishing) is particularly dangerous. In a spear phishing attack, scammers use a company's real logos, names, and terminology and may even spoof real email addresses in order to create convincing phishing emails to trick that company's employees. For example, previous spear phishing attacks on the University community have used terms like "UDelNet" and logos like the interlocking UD in official-looking fake emails.

Avoid falling victim to phishing scams. Always verify that the sender is legitimate and that the links go to trustworthy domains. Look for mistakes in the information or wording of the email. If you have questions about the email's content, contact the alleged sender through a separate channel. You can also check the [**Secure UD Threat Alerts**](https://sites.udel.edu/threat/) blog to see if the email has been identified as a known scam.

If you receive a phishing scam, forward it to reportaphish@udel.edu and then [**erase**](https://www1.udel.edu/security/phishing/erase.html) it.

**7. How can I protect myself from identity theft?**

Protecting yourself from identity theft is largely a matter of following best practices (and requirements) for information security. If you learn to identify and avoid [**phishing scams**](https://www1.udel.edu/security/phishing/) and [**install and run anti-virus software**](https://www1.udel.edu/security/bestpractices/avs.html), you'll protect yourself from the most common means by which hackers and scammers steal your personal information. Exercise caution when providing personal information, including your name and date of birth, Social Security number, and bank account or credit card numbers, to anybody. If you're providing this information online, make sure that you're using a secure form and connection and that you're on the legitimate website of the company or group you mean to contact.

You can also request [**credit monitoring**](https://www1.udel.edu/security/bestpractices/identity.html) to watch for suspicious activity on your credit files.

**8. What kinds of information are safe to share on social networking sites?**

When you use a personal account on a [**social networking site**](https://www1.udel.edu/security/bestpractices/socialnetworking.html), you are in control of the information you share, including what you share and who can see it.

Limit the amount of personal information you share through your social networking sites. For example, consider whether you need to share your date of birth, hometown, birth town, the names of pets, etc. While this information may sometimes be interesting to friends, it's also the kind of information most often asked for by security questions, and attackers can potentially use the information you post on your social media accounts to impersonate you or bypass some kinds of authentication procedures.

Remember, too, that any information you share on the internet can be shared by others. Once you post something, you can't necessarily delete it; sharing and archiving features make it so that your information persists online, sometimes in unsafe locations. Personal photos in particular are often propagated, so think twice before posting a picture of yourself that you wouldn't want friends, family, or employers to see.

Check your account's privacy and sharing settings and limit who can see your posts and personal information. For example, you may choose to censor certain personal information such as your birthday so that only people on your friends list can see it. Think about whether you need location services turned on or whether you want other people to be able to tag you in photos.

**9. How should I use University social networking accounts?**

When you use a University account of any type, including an official [**social media**](https://www1.udel.edu/security/bestpractices/socialnetworking.html) account, you are both expected and obligated to use it according to the conditions under which it was provided to you. Don't use official University accounts for personal purposes. Share only the information that you are authorized to share through that account, and do not use the account to post your personal opinions or endorse ideas outside of the University's official capacity. For example, don't use your unit's social networking account to like a band or share a political opinion.

If you're unsure of whether something is acceptable, ask your supervisor or refrain from doing it. Remember, official University accounts represent official University views. Don't take actions that will reflect poorly on the University; save your personal use for your personal accounts.

**10. Am I allowed to use my personal device for University activities?**

The University does not prohibit the use of personal devices for University activities. If you're considering using your own computer or mobile device for work, consult your unit head or local support provider to discuss the potential risks to both University and personal information and whether a personal device is appropriate for the task.

Be aware that all devices—personal or University-owned—used to conduct University activities are held to the University's information security standards.

**11. Am I allowed to download music, movies, and other media?**

Only if you're doing it [**legally**](https://www.udel.edu/legaltunes/).

There are lots of artists and companies producing music, games, television shows, movies, software, and other media. This media is protected by [**copyright laws**](https://www1.udel.edu/security/copyright.html) such as the Digital Millennium Copyright Act. Anybody who violates copyright laws by illegally downloading copyrighted material is subject to fines and other legal action.

To facilitate the exchange of scholarly information, the University does not restrict or filter network traffic. Your access to the University network does not, however, give you license to violate copyright laws. The University will cooperate with copyright holders to identify individuals who illegally share copyrighted materials.

Do not illegally download copyrighted material. Remove [**peer-to-peer (P2P) file-sharing programs**](https://www1.udel.edu/security/bestpractices/p2p.html) from your computer prior to coming to campus, and do not facilitate illegal file sharing or torrenting.

**12. Am I allowed to used my University-owned device to play games, listen to music, or browse the internet?**

Employees are given access to University-owned devices for work purposes. If you have a question about a non-work or otherwise unusual use for your University-owned device, consult your unit head or local support provider to discuss the potential risks to both University and personal information and whether the proposed use is [**acceptable**](https://www1.udel.edu/security/bestpractices/acceptableuse.html).

For example, you may not use a tablet in a healthcare clinic to play games or listen to music between appointments.

As a general rule, you shouldn't install apps or enable functions on a University-owned or -operated device unless they're [**essential**](https://www1.udel.edu/security/bestpractices/functionality.html) to the work-related tasks you're performing.