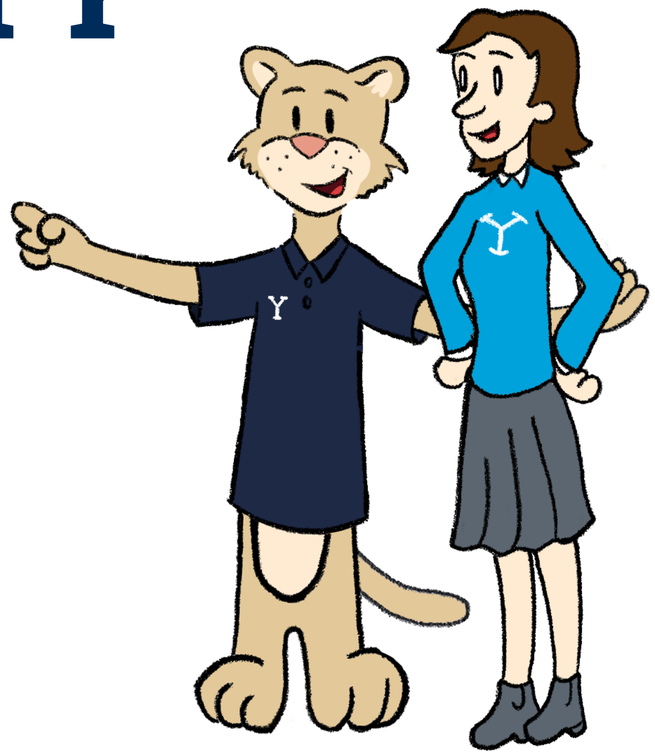
BYU | OFFICE OF INFORMATION SECURITY

We might have the office, but

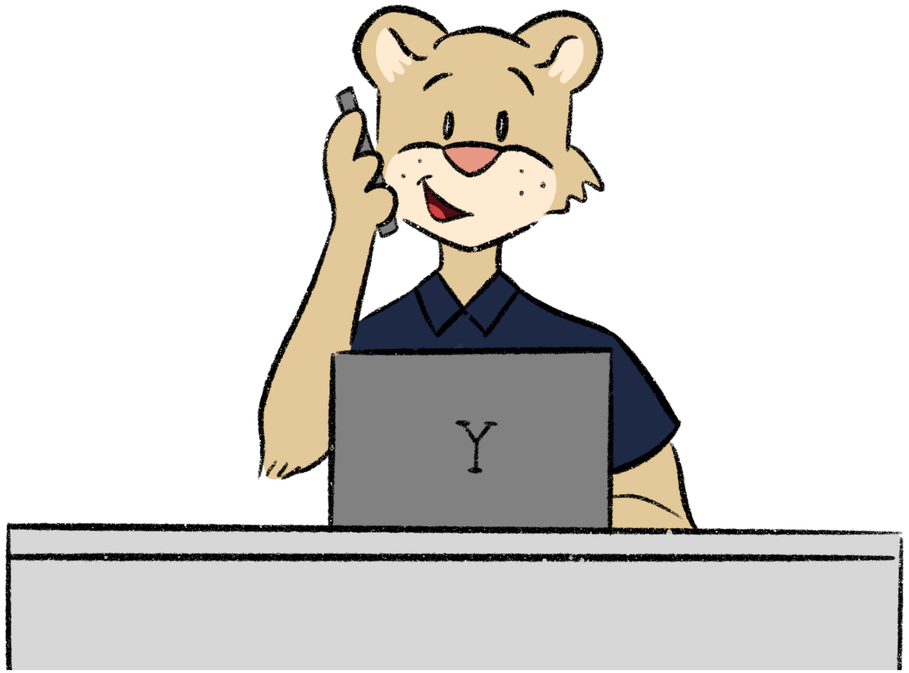
INFORMATION SECURITY starts with you.



Welcome! You are part of a great workplace and community in which you will have many rewarding experiences. As part of the BYU family, we all share the responsibility to guard and protect personal information and our information systems from others who would attempt to access or use this information without authorization. We're sharing important tips that will help you secure your information and that of the university. Check out the topics below to get started.

INTRODUCTION

Why are we talking about Information Security?



Over the years, educational institutions, including BYU, have been a growing target for cybercriminals. In order to function efficiently and serve our community, we use personally identifiable information including financial data, medical information and Social Security numbers. The university also generates important information and data from research projects. It's vital that we work together to protect and safeguard this valuable information.

Being proactive with your information security protects your computer and personal information and in turn, helps keep the university safe and secure. Each of us can be a target, which is why it's important to always maintain healthy habits of information security.

PASSWORDS

When “cougar1234” isn’t enough anymore

Having a strong password is often your first line of defense against a hacking attempt. Creating strong passwords for your various accounts is essential in protecting your identity, accounts, and network security. Weak passwords can make you an easy target for hacking, but so can poor password hygiene.

To help you protect your identity, accounts, and network security, follow these guidelines:

- Use strong passwords
- Don’t share your password with anyone
- Use character substitutions (“o” with “0,” “a” with “@”)
- Use a different password for each website or service you use
- Don’t recycle passwords
- Don’t use birth dates, pet names, or other personal information
- Add security questions for password resets

To change your password or to add security questions follow the instructions here.

What Makes a Strong Password?

Passwords must be at least 8 characters. However, the shorter you make your passwords, the more complex they need to be to stay strong.

- **8-11 characters** - use uppercase and lowercase letters, symbols, and numbers
- **12-15 characters** - use uppercase and lowercase letters and numbers
- **16-19 characters** - use uppercase and lowercase letters
- **20+ characters** - use any characters you want

DUO MOBILE

A wingman for the digital age

Multifactor authentication is another crucial defense against hacking and should be used whenever possible. Multifactor authentication, or two-step verification, requires authentication through a second device. Duo is a two-step verification service that BYU requires for most of its websites. Like other multifactor authentication services, Duo strengthens security and protects against hackers.

Click here to enroll in Duo Mobile

1. Open Duo
2. Click "Enroll"
3. Fill in your BYU username and password
4. Click "Start Setup"
5. Add your device and follow the instructions for installing Duo

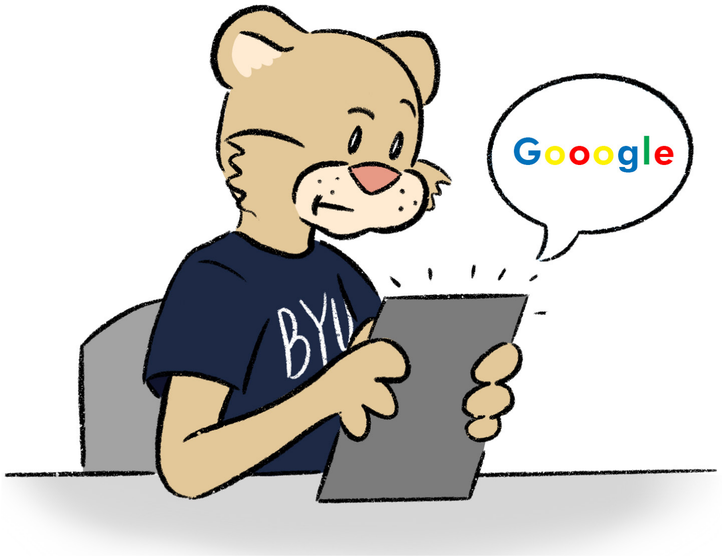
PHISHING

An email from Twittter is not from Twitter.

Phishing is a way people try to log in to your accounts and get your private information. Phishing is a form of spam that can be tricky to identify because the sender of the email often poses as a trusted authority in order to acquire sensitive, personal, information about you. This information can even include things as confidential as your Social Security number or bank information!

Though phishing can come in many forms, the three most common types of email phishing are described below.

1. **Credential Hunting and Harvesting** – Hackers try to gain access and control of your credentials—usually your username and password—to log in to your various accounts and steal private information or to amass large quantities of credentials to sell.
2. **Scams** – Scammers want your personal, financial, or other sensitive information and will try to trick you. If an email offer is noted as "urgent" or seems too good to be true, it is probably a scam.
3. **Malware** – Hackers send links or attachments that are programmed with malware or viruses. Clicking on the link or attachment allows hackers to take over your computer.



Tip: The best defense against phishing is to avoid clicking on links, downloading attachments, or entering personal information in any email you were not expecting, even if it's from someone you know.

Report suspicious e-mails to abuse@byu.edu.

ANTIVIRUS

Your computer's very own can of pepper spray

Anti-virus software protects against viruses used by hackers to take control of your computer or to get personal information. Install anti-virus software now or, if you have it installed, make sure it's updated.

Be sure to research the software for legitimacy as malware will often disguise itself as anti-virus software. Anti-virus software is downloaded onto a computer, often at a cost, and instructions will differ slightly depending on which anti-virus software you decide to use. For download links and information on security software, visit infosec.byu.edu.

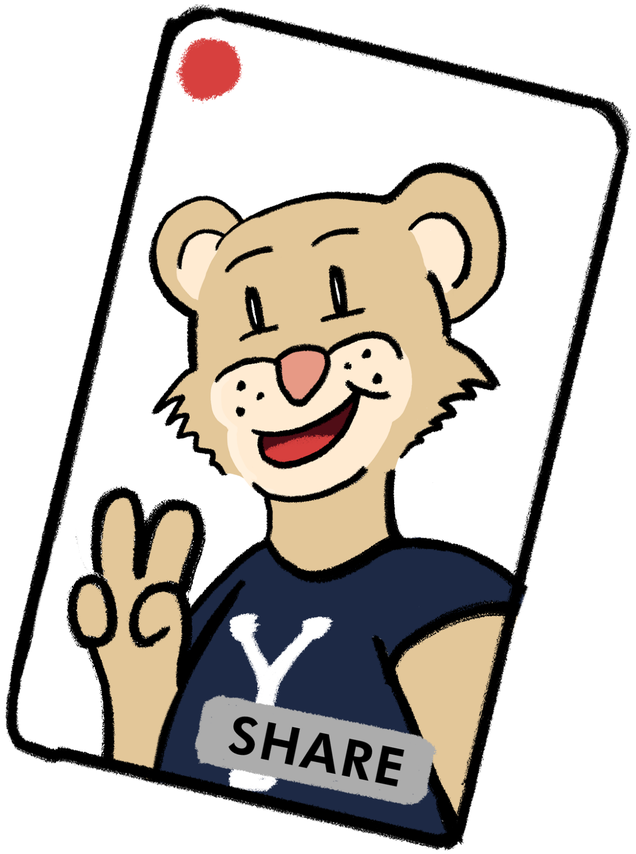
SOCIAL MEDIA

Keep your friends close and your enemies distant

Social media sites are a useful attack tool for hackers, simply because of the amount of personal information present on social media. Of course, it is nice to stay connected to friends through Facebook, Instagram, and Twitter or to find a job opportunity through LinkedIn, but make sure the way you are connecting isn't compromising any of your sensitive personal information.

Following these tips can help you protect your personal information:

- Be aware of the information you share on social media. Never share personal or sensitive information about you (or others) on social media.
- Know your network. Are the people you don't personally know credible, safe sources of information?
- Consider the consequences of your posts. **Always** think about what you are posting before you post it.
- Adjust privacy settings to limit the amount of information you share.
- Create secure passwords.
- Log out when you're done.
- Be cautious when clicking on links.



WI-FI CONNECTIONS

They ask, “Wi?” and you say, “Wi-Fi not?”

Make sure that you use a secure Wi-Fi network as often as possible. Secure wireless networks are password protected. Use Eduroam or BYUSecure whenever available.

Eduroam is a nation-wide multi-institutional secured network. Your Eduroam login credentials can be used across the nation at any and all Eduroam-supported institutions. A primary benefit of Eduroam is that it gives visitors from other universities an easi-ly-accessible encrypted Wi-Fi option to use while visiting other Eduroam-supported campuses.

For information on Wi-Fi options, including Eduroam, go to the BYU Wireless Network page.

SECURITY INCIDENTS

After taking all available security precautions, it's important to continue being vigilant in monitoring your accounts. Regularly check your personal financial accounts, school accounts such as MyBYU and My Financial Center, and social media and entertainment accounts for suspicious activity.

If you suspect or know that an incident has occurred, follow these steps:

1. Immediately contact us by calling 801-422-7788 or emailing us at cessoc@byu.edu. Do NOT try to remediate the incident on your own.
2. Report the incident to your management chain.
3. Disconnect the computer or device from the network to stop/minimize any potential external hack or loss of data.
4. Keep the device on and running-do NOT turn off or restart your device. This will help preserve the current state of the system.
5. Do not continue to use the device.
6. Cooperate with any analysis or investigation that may follow.

Remember: Information security incidents are part of our current environment and can happen to anyone. If you are unsure whether an event is a security incident, it is best to reach out and report the event.

In the case of physical threats or theft of equipment, report the incident to the police. If a university device or a personal device storing sensitive university information is involved, notify the OIT service desk as well.

On-campus Police: (801) 422-2222 OIT Service Desk: (801) 422-4000

TO LEARN MORE ABOUT INFORMATION SECURITY, VISIT infosec.byu.edu