



# What is Information Security Awareness?

The University of North Carolina at Chapel Hill protects its data network from thousands of daily intrusion attempts by potential hackers, but technical protections alone are not sufficient. Employees are the most important component in protecting the confidentiality, integrity and availability of University information by following safe computing practices.

This training will introduce basic security awareness concepts and strategies you can use at work and at home.

# About this Module

In this module, you will learn:

1. About sensitive, University-owned information;
2. How to report an information security incident if it occurs; and
3. Easy strategies you can use to protect your computer.

# What is sensitive information?

Sensitive information is often protected by law and/or University policy.

Examples of sensitive information may include:

- Full Social Security numbers
- Credit card numbers
- Driver's license numbers
- Passport numbers
- Human research subject information with real names
- Medical information with names or other identifying information
- [And more...](#)

# What can you do to protect sensitive information?

- If you work with sensitive, University-owned information via your computer, ask your technical support staff if appropriate protections are in place. If you do not have local technical support, please don't hesitate to contact the Information Technology Response Center (ITRC) at 919-962-HELP or 1-866-962-4457 (US and Puerto Rico). The ITRC may refer you to the University Information Security Office for some types of questions.
- If you are the system administrator for a UNC-Chapel Hill server that works with sensitive, University-owned information, make sure the server is registered for the System Administration Initiative (SAI):
  - <http://help.unc.edu/help/systems-administration-initiative-sai-overview/>

# To Report a Security Incident

- If you believe sensitive, University-owned information is in danger:
  - Without delay, call the ITRC at 919-962-HELP (24 hours a day, 7 days a week).
- The ITRC may refer you to an Information Security Office incident handler. If so, don't forget to provide a telephone number at which an incident handler can reach you.
- If your report is referred to the Information Security Office, DO NOT try to fix the problem. Stop using the computer until you receive a call from an incident handler (generally within 30 minutes).

*If you lose a University-owned, mobile device,  
notify your supervisor and campus police (919-962-8100) immediately.*

# 7 strategies for protecting sensitive information

1. Recognize PHISHING when you see it
2. Use strong passwords and diversify them
3. Update your software regularly
4. Install and use supported anti-virus software
5. Configure firewall software to run on your computer
6. Use Virtual Private Network (VPN) connections to UNC-Chapel Hill when off-campus
7. Lock the display on your computer

# 1. Recognize PHISHING when you see it!

**What is Phishing (pronounced 'fishing')?** Emails, phone calls, or text messages sent by criminals posing as legitimate businesses or organizations for the express purpose of gaining access to your confidential information such as passwords, account numbers, your birth date or social security number.

*Example of a phishing email:*

From: First Generic Bank <accounts@firstgenericbank.com>  
Subject: Please update your account information  
Date: Sep 12, 2006 3:23 PM PST

---

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit <http://www.firstgenericbank.com.account-updateinfo.com>.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,  
First Generic Bank

# PHISHING (cont)

- **What should I do if I get a suspicious communication?**
  - Don't respond! Responses only increase the likelihood of phishing continuing.
  - Report it at <https://help.unc.edu/help/how-to-report-phishing-and-spam-emails/>
- **What should I do if I mistakenly click on a link in a suspicious communication?**
  - Contact the ITRC at 919-962-HELP. They will help you determine if any actions need to be taken.

Phind the phish





## 2. Use strong passwords

There are many strategies for creating strong passwords. Here are a few of our favorites:

- Don't use words that can be found in a dictionary.
- Don't use your name, your child's name, or your pet's name or anything about you that can be discovered on the Internet.
- Consider using a passphrase. Passphrases are a string of words, like a quote, that you can remember. For example, "Comedy is simply a funny way of being serious." This can be converted to CISAFWOBS. Now you can vary the capitalization, add some special characters (+,{“&) and numbers to create your password: 3+7CISaFWoBS=10
- Use different passwords for different kinds of accounts.

*Protect your passwords by preventing your web browser from “remembering” sensitive passwords like Onyen or bank accounts.*

# Passwords should NOT:

- Contain more than three characters from the user's account name,
- Contain your birthdate or information discoverable about you on the Internet,
- Be shared with anyone,
- Be used for multiple accounts,
- Be put on a sticky-note under your keyboard,
- Be "remembered" by your browsers.
  - Instructions regarding how to delete passwords from you browser:

<https://help.unc.edu/help/how-to-remove-saved-passwords-from-a-web-browser/>

### 3. Update your software regularly

Intruders can leverage computer software vulnerabilities to break into your system. To resolve the vulnerabilities, keep your computer up to date with needed software patches.

- The ITRC provides instructions on how to update your operating system, web browser, or web applications (Java, Acrobat, Flash):
  - <https://help.unc.edu/help/update-your-software-regularly/>

**Qualys BrowserCheck:** This tool can help you identify and resolve browser vulnerabilities.

- <https://browsercheck.qualys.com/>

## 4. Install and use antivirus software

Computer viruses are spread through Internet links, email attachments, and a variety of other means, all with the intention of recording, corrupting, changing or deleting data on your computer.

**Antivirus software** scans your computer on a schedule you set to detect and disable or remove viruses and other harmful applications.

- Make sure your UNC-Chapel Hill owned computer(s) are running University-provided antivirus, if available. Your local technical support staff or the ITRC can help you with questions.
- Microsoft Security Essentials is available to all employees in support of properly secured home computers. With an active Onyen faculty, staff, and students can download it for free at:

<http://shareware.unc.edu>

## 5. Install and use firewall software

**Firewall software:** A firewall assesses traffic entering (and leaving) your computer and compares the traffic to rules intended to stop unwanted traffic. All major operating systems, such as Windows and Mac, have a built-in firewall. Making sure your firewall is turned on is one of the best steps you can take to secure your computer.

Carolina Computing Initiative (CCI) computers come with the firewall activated.

Check with your technical support but you may be able to determine if the firewall on your system has been activated by checking here:

**Need help figuring out if the firewall in your computer has been activated?**

- <https://help.unc.edu/help/how-to-enable-a-firewall-on-windows-and-mac-os-x/>

## 6. Use the VPN when off-campus

UNC-Chapel Hill invests heavily in ensuring the security of the campus data network. When you need to access the campus network from off-campus, VPN (Virtual Private Network) software connects you as securely as if you were on campus.

The VPN software can be obtained for free from <https://vpn.unc.edu>


**Wireless Access:** When using a wireless device on campus, **UNC-Secure** is the preferred network connection. <http://help.unc.edu/help/connecting-to-the-unc-wireless-network/>

*Contact your local technology support or the ITRC  
if you need help setting up a VPN connection.*

# 7. Lock your computer

When you leave your desk/computer, even for a few minutes, an opportunity is created for someone to access your account and any sensitive information you see via your computer. If you don't already lock your computer when you step away from it, doing so is a quick and easy practice for securing your computer from people who might be able to see your display/monitor.

## How to lock a Windows machine:

- Hold down the  + L key at the same time or depress Ctrl-Alt-Delete at the same time

## How to lock a Mac:

- From System Preferences, select Security, then General.
- Select “Require password immediately after sleep or screen saver begins.”
- Select System Preferences, then Desktop & Screen Saver, then Screen Saver and select 10 minutes.

*Locking your computer can also prevent someone from taking actions on your computer.*



## For more information:

To learn more about UNC Chapel Hill Information Security Policies:

- <http://its.unc.edu/about-its/university-it-policies/>

### **ITRC Contact Information**

- Walk-in assistance is available in the basement of the Undergraduate Library
- For telephone assistance, call 919-962-HELP (4357) or toll free 1-866-962-4457
- For assistance via instant messaging: contact [Live Chat service](#)
- For email assistance, please submit an online [Help Request](#)