Information Technology Department

Computing Security Awareness

Why should I be concerned?

Think about everything you use your computer and mobile device for and the access you have to information on them. Then consider how much personal and sensitive information – financial data, educational records, employee records, social security numbers, and more - that Franklin Pierce maintains on students, faculty, and staff on computer systems. Without good security practices, data can be exposed, modified, deleted, or stolen resulting in institutional loss of trust and reputation, money, and productivity as well as significant legal ramifications.

You may say "Isn't computing security just an IT problem?" The answer is no. Good security standards follow a "40/60" rule, 40% of security safeguards are technical and 60% rely on computer users like you adhering to good security practices.

What does this mean for me?

This means that everyone who uses a computer or mobile device with access to the Franklin Pierce network needs to understand how to keep data secure. This includes being familiar with University policies and best practices related to information security. In particular, you should be familiar with the Information Security Policy and, if you are an employee, the Technology Acceptable Use Policy for Employees.

Franklin Pierce is also obligated to comply with federal regulations including FERPA (protecting the privacy of student educational records) and HIPAA (protecting the security of health information). Ask your supervisor about how these regulations may apply to your job.

What are security threats?

The severity and range of threats to information security are vast and increasing every day. The most common threats include:

- **Malware** – an umbrella term for all malicious software including computer viruses, ransomware, spyware, adware, etc. that is designed to infiltrate or damage computers or intercept personal data without the user's consent. Some malware is relatively innocuous, such as causing messages to appear on your screen, but others can be destructive, such as locking up your files or wiping out your hard drive. Malware can also be unknowingly passed on to others through emails and file sharing.

- **Application Exploits** – weaknesses in application software (such as web browsers, Adobe PDF reader) or in the operating system software which can be exploited by cybercriminals to infect your computer with viruses or other malware.

- **Weak Passwords** – passwords that are short, simple, or readily associated with you that are easy to detect by someone else or through "password-cracker" programs. Examples of weak passwords include family member names, birthdays, town or street names, and even dictionary words or words spelled backwards.

- **Social Engineering** – or "phishing" is typically a non-technical scheme to trick you into revealing personal information such as passwords or bank information or giving up control of your computer. This may take the form of an email that appears to be from a friend or a web site that looks legitimate but contains a link to download a file or request private information. It may also be a threat indicating that you must act quickly or that you must forward the email to someone else. Other social engineering threats can include telephone calls or face-to-face interactions from individuals purporting to be someone they are not.

What can I do?

This is not an exhaustive list but following the best practices below will greatly minimize your computing security risks:

- Ensure your computers anti-malware (and specifically anti-virus software) is active and up-to-date on all computers that you use to access University data (anti-malware software is installed and automatically updated on Franklin Pierce computers connected to the network).
- Create strong passwords (use upper and lower case letters, numbers, and special characters and make your password at least 8 characters. Using a phrase like "This May Be One Way to Remember" to create the strong password "TmB1w2R!" may be helpful).
- Never share your password with anyone else.
- Never re-use your Franklin Pierce account password for personal accounts.
- Never re-use passwords for the same account. Create a new password for each new password request (if you need to write them down, store them in a locked cabinet or drawer for which only you have access).
- Avoid auto-saving passwords on web sites.
- Password-protect your mobile device.
- Configure your mobile device to automatically lock the screen after a short period of inactivity.

- Don't open or reply to emails from unknown sources. It is best to **delete** them.
- Avoid emails that are not addressed to you specifically by name.
- Don't assume that email, instant messages, texts, or attachments are confidential.
- Don't click on unknown or unsolicited links or attachments and don't download unknown files or programs. Don't click on links in pop-up windows.
- Don't open e-mail attachments or go to embedded url address links even when they seem to be from people or businesses you are familiar with unless you are confident that the intent is valid and safe. Be especially wary of messages or titles with misspellings or odd grammar.
- Avoid unknown web sites that offer special or free deals or promises that are too good to be true.
- At a minimum, look for "https" at the beginning of the url or site address before entering any sensitive information or password (the "s" indicates there is a "secure" connection).
- Avoid revealing confidential or sensitive information on social media sites (a good rule of thumb is to only post information that you would be willing to put on a banner in a public place).
- Don't store sensitive files on your computer's hard drive or on flash drives as these files are not typically backed up and flash drives are easily lost or stolen. Keep in mind also that if you are using a laptop and the laptop is lost or stolen, so is the data on it.
- Don't connect external storage devices from untrusted sources to your computer (for example, if you find a flash drive in the parking lot or elsewhere, don't plug it in your computer – that's a popular social engineering attack).
- Use a "data destroyer" to delete sensitive files on your computer. Using the Delete function doesn't actually delete the data. Contact the IT Help Desk for recommendations.
- Log out or lock your computer (Windows key + L) when stepping away from it for even a short period of time and always save your work and log out at the end of the day.
- If you suspect a security breach or have questions, contact the IT Help Desk at ithelpdesk@franklinpierce.edu or 603-899-4214.

Some of this content was adapted, with permission, from the **Computing Security Awareness** presentation developed by the Information Services and Technology Department at Boston University.