Protecting our information

Helping to keep the information we use everyday, safe and private, is up to everyone in our campus community. Although we have a very capable IT staff, we can help the process by being aware of many of the threats we face on-line and understand what we can do to help keep our data from unauthorized use.

Data Privacy Month is a reminder to review our practices and adjust to the changing threats we face.

One of the most common threats we face on-line, is “phishing.”

What is Phishing?
Phishing is a social engineering scam whereby intruders seek access to your personal information or passwords by posing as a legitimate business or organization with legitimate reason to request information.

Types of Phishing

- **Email Phishing** with email and spam is a very common phishing scam. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change details, and verify accounts.
- **Spear phishing** is an attack that targets a specific individual or business. The email is addressed to you and appears to be sent from an organization you know and trust, like a government agency or a professional association.
- **Whaling** is a phishing or spear phishing attack aimed at a senior official in the organization.

How to protect yourself against “phishing”
NEVER provide your password to anyone via email.

Be suspicious of any email that:
- Requests personal information.
- Contains spelling and grammatical errors.
- Asks you to click on a link.
- Is unexpected or from a company or organization with whom you do not have a relationship.

If you are suspicious of an email:
- Do not click on the links provided in the email.
- Do not open any attachments in the email.
- Do not provide personal information or financial data.
- Contact the Technology Support Center 570-941-4357

PASSWORDS
Create Strong Passwords:
- Use nine or more characters - Caps, numbers, and symbols mixed in
- Passwords should be hard to guess and avoid dictionary words
- Never divulge your password to anyone in an email
- Change your passwords often
- Use good passwords with strength appropriate for the importance of the site
- Banking website passwords should be stronger than a forum site
- Use different passwords for different websites or types of websites
  - Online Banking
  - Personal Email
  - Online shopping
  - Social media: Facebook, Twitter, LinkedIn, Pinterest

DO NOT use your University of Scranton password for any other login!

Security Questions
What makes a good security question? The answer to a good security question has the following criteria:

- Safe: cannot be guessed or researched
- Stable: does not change over time
- Memorable: can remember
- Simple: is precise, simple, consistent
- Many: has many possible answers

Recommended Anti-Malware Programs for Personal Use:
(Note: All of the anti-malware tools we endorse are suited for personally owned, non-university devices only. These programs should not be installed on University of Scranton managed devices.)

Malwarebytes Anti-Malware (PC): www.malwarebytes.org
Spybot - Search and Destroy (PC): www.safer-networking.org
Ccleaner (PC or Mac): www.piriform.com
Adblock Plus (PC or Mac): www.adblockplus.org
Ghostery (PC or Mac): www.ghostery.com/en/
Trend Micro Mobile Security: For Android For Apple iOS
Safe Web Browsing Tips:

It is very easy to clone a real website and does not take a skilled developer long to produce a very professional-looking, but malicious site.

- Use your instincts and common sense.
- Check for presence of an address, phone number and/or email contact – often indications that the website is genuine. If in doubt, send an email or call to establish authenticity.
- Check that the website’s address seems to be genuine by looking for misspellings, extra words, characters or numbers or a completely different name from that you would expect the business to have.
- Roll your mouse pointer over a link to reveal its true destination, displayed in the bottom left corner of your browser. Beware if this is different from what is displayed in the text of the link that brought you to this page.
- If there is NO padlock in the browser window or ‘https://’ at the beginning of the web address to signify that it is using a secure link, do not enter personal information on the site.
- Websites which request more personal information than you would normally expect to give, such as user name, password or other security details IN FULL, are probably malicious.
- Avoid ‘pharming’ by checking the address in your browser’s address bar after you arrive at a website to make sure it matches the address you typed. This will avoid ending up at a fake site even though you entered the address for the authentic one – for example ‘eeyebay’ instead of ‘ebay.’
- Always get professional advice before making financial decisions. Sites that hype investments for fast or high return – whether financial or for commodities – are often fraudulent.
- Be wary of websites which promote schemes that involve the recruitment of others, receiving money for other people or advance payments.
- Be wary of websites that are links in unsolicited emails from strangers.

Malware

What is Malware?

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, or it may be designed to cause harm, often as sabotage (e.g., Stuxnet), or to extort payment (CryptoLocker).

How does Malware infect computers?

- Email
- The Internet
- Outdated software
- Peer-to-peer (P2P) file-sharing systems
- Social networks
- Pop-ups
- Computer storage media
- Mobile devices

How Is Malware removed?

There are many anti-malware products available for the general public. Some are better than others, and care must be taken when choosing an anti-malware program for download. This is one of the most common places where malicious actors lure unsuspecting users into downloading malware, with users thinking they are helping their situation.

The University has a process in place to help deal with malware removal. If your university-owned computer is detected to have a virus, it will be immediately dropped from our networks. The user will then be notified to contact the Technology Support Center in Alumni Memorial Hall for further instructions. In many cases this process may result in loss of your existing file information and will result in a substantial delay in getting your computer back to normal.

Need Additional Help?
E-mail the Technology Support Center:
techsupport@scranton.edu
Or call 570-941-HELP (4357)