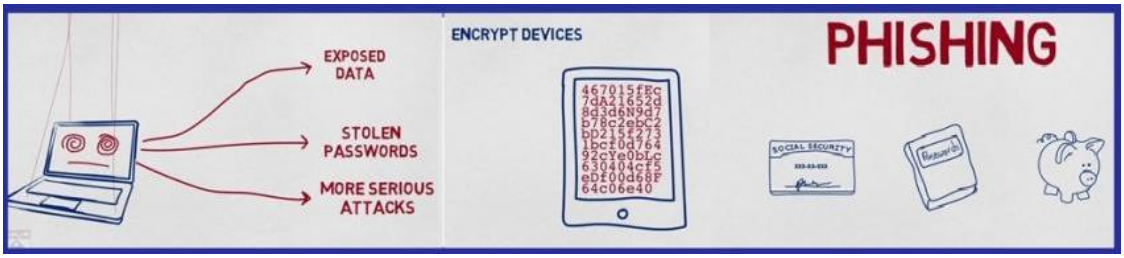
ITS Tipsheet #1

Top 10 Information Security Tips

It is imperative that all Penn employees take appropriate steps to protect Penn's computing infrastructure, user accounts, and data. As a follow-up to the *ISC Information Security Essentials Online Training*, this Tipsheet provides the top ten steps you can take to protect your personal information and the university's technology assets.



1. **Don't click on links in unexpected or untrusted emails.** An email from someone you don't know or don't expect to receive a message from prompting you to take an urgent action is most likely a phishing scam.

2. **Install anti-virus software on your home computers.** Penn offers anti-virus software for students and staff at no cost. Visit https://www.isc.upenn.edu/how-to/antivirus-desktops-and-laptops.

3. **Use complex passwords.** You can always check the complexity of your PennKey password by clicking on "Test My PennKey" at the PennKey home page: http://www.upenn.edu/computing/pennkey/index.html.

4. **Browse trusted websites for business purposes only.** Avoid clicking on ads or pop-up windows when browsing. Never allow you browser or a website to remember your password.

5. **Use a password manager app.** Too many passwords to remember? Use the LastPass password manager app on your smartphone. Visit the Penn-LastPass page at: https://www.isc.upenn.edu/how-to/lastpass.

6. **Don't store Penn data on an unencrypted personal device such as a laptop or tablet.** If you are not sure where to store data and sensitive files, contact ITS for assistance.

7. **Report a lost or stolen Penn computer or mobile device to the ITS team as soon as possible** – don't delay.

8. **Don't use untrusted flash/portable media.** Never use flash drives given out at conventions or provided by salespeople.

9. **Use special care when handling or storing regulated data**, such as student information, social security numbers, credit cards and health data.

10. **Never share your password** – *with anyone.*

REMEMBER: ITS will never ask for your PennKey password.

Receive a suspicious email, or just aren't sure if an email you received is a potential phishing attempt? Contact the ITS helpline at x8-HLPU.

WHAT IS PHISHING?

A "phishing" attack is when a criminal sends an email pretending to be someone (ex. your manager) or something they are not (ex. Google), in order to extract sensitive information out of the target.

ANTI-VIRUS SOFTWARE HAS LIMITS

Anti-virus software usually cannot prevent or detect a phishing attack.

DATA BREACHES CONTINUE TO RISE

According to Risk Based Security's 2017 Data Breach QuickView Report, there were 5,207 breaches recorded last year around the world, surpassing the previous high mark by nearly 20%, set in 2015. The number of records compromised also surpassed all other years, with over 7.8 billion records exposed, a 24.2% increase over 2016's previous high of 6.3 billion.