ITS Tip Sheet #2

Password Management

Easy steps you can take to protect your accounts and Penn's information assets

THE RISING COST OF DATA BREACHES

On average, it costs higher education institutions $245 for *each data record* that is compromised[2]

HIGHER ED: DATA BREACH TARGET

17% of all data breaches happen in higher education – second only to the healthcare industry[3]

- Your "PennKey" is a combination of your PennKey user name and password
- Report compromised PennKeys immediately to Information Security at: security@isc.upenn.edu or by phone to 215-898-2172
- Consider occasionally changing your PennKey password
- Use a password manager app on your smartphone to store all of your passwords in one place for easy reference

Compromised passwords create one of the largest information security risks within any organization. In the first half of 2017, reported data breaches in higher education more than doubled[1]. The most common way passwords are compromised is through targeted "phishing" attacks where an end user clicks on a malicious web link, typically received in email. A user is then taken to what appears to be a legitimate website and unwittingly enters an account name and password.

Remember: Neither ITS nor ISC will ever ask for your PennKey information. Only you will ever know your PennKey information. PennKey information is stored in an encrypted form. It is not accessible or readable by anyone else, even IT system administrators.

Following the advice contained in this tip sheet will help to prevent misuse of your system accounts and compromise of Penn's information assets.

☞

ITS Tip Sheet #2

Password Management

5 Tips for Managing Your Passwords

1. Never, under any circumstances, share your PennKey information with anyone. IT staff on campus will never ask for your PennKey information.

2. Choose unique, complex passwords only. Your password must meet the following criteria:
   - ***LONGER PASSWORDS HAVE FEWER COMPLEXITY REQUIREMENTS***
   - 20 characters: any combination of keyboard characters
   - 16-19 characters: must contain caps and lower case letters
   - 12-15 characters: must contain caps, lower case, and numbers
   - 8-11 characters: must contain caps, lower case, numbers, and symbols
     - capital letters (A,B,C…)
     - small letters (a,b,c…)
     - numbers (0,1,2,3…)
     - symbols (!,#,$...)

   You can always check the complexity of your PennKey password by clicking on "Test My PennKey" at the PennKey home page: https://challengeresponse.apps.upenn.edu/challengeResponse/jsp/fast.do?fastStart=pennkeyTester

3. Download the **free** LastPass password manager app for your smartphone. To learn more about using LastPass, visit the Penn-LastPass page at: https://www.isc.upenn.edu/how-to/lastpass

4. You can change your PennKey password at any time at: https://weblogin.pennkey.upenn.edu/changepassword

5. Never use the same password for multiple systems.   Avoid using similar or sequentially numbered passwords, i.e: P@ss2020! *and* P@ss2021!

References

1. Campus Technology, https://campustechnology.com/articles/2017/09/20/education-data-breaches-double-in-first-half-of-2017.aspx
2. Education Advisory Board, https://www.eab.com/daily-briefing/2017/07/27/cost-of-data-breaches-in-education-hits-all-time-high-$245-per-record
3. HUB International, https://www.hubinternational.com/blog/2017/03/higher-education-university-data-breach/