Why Good Password Practices Are Important

Protecting Our Community

- Students and families entrust us with their information.
- Collectively, our databases hold the information of tens of thousands of individuals.
- Most people underestimate the impact of compromised data, identity theft, and other security issues — Our good practices help shield them from genuine catastrophe.

Protecting Our College

- Luther can be held financially and legally accountable.
- We trust our coworkers — many successful attacks exploit that trust. One person's poor password practices affect many.
- Many systems are linked or contain information that can help compromise other systems.

Protecting Ourselves

- Many of us have personal information inadvertently pass through our work accounts.
- Many important assets are work related: e.g. 401k, Health information, Life Insurance.
- Things that happen under your account — Spam, file destruction, etc.— all have *your* name tied to them.

How Password Integrity is Threatened

Phishing

- An attack where you "take the bait" by clicking a link, opening an attachment, or filling a form designed to access your account or steal information.
- Phishing can happen in various contexts: email, web, even over the phone.
- Phishing attacks can seem very genuine, even including Luther logos, offices, and other info.

Malware

- Broad term for viruses, adware, spyware and other files that infect a system.
- Malware's effects range from showing specific ads to logging your keystrokes to holding data hostage for millions of dollars.
- Malware and Phishing are often linked.
- All devices are susceptible.

Personal & Institutional Habits

- Most people only have two or three weak passwords that they use for everything.
- Shared passwords should change whenever an employee leaves.
- Avoid storing passwords on a spreadsheet or document.
- Never send passwords digitally.

LUTHER COLLEGE
Information Technology Services

Changes We're Making as an Institution

Revised Norse Key Policies

- New restrictions on passwords have already taken effect.
- Must not contain these special characters (\ * : , < >)
- Allows Colleague to be linked to Norse Key, reducing number of passwords and thus exposure.
- Only affects new passwords.
- See *norsekey.luther.edu* for specific rules.

Password Manager Pilots

- Password Managers can generate extra strong passwords, store them securely, and allow them to be shared and managed safely.
- Highly recommended in your personal life.
- Piloting at Help Desk and in ITS.
- Medium-term change affecting employees.

Two Factor Authentication

- Two-Factor Authentication requires confirmation from a different device in addition to a password.
- Drastically more secure.
- Seeking to add to Norse Apps (email, etc).
- Medium-term change affecting many people.

Changes You Can Make as an Individual

Strong Passwords

- The best source of password strength is length.
- Strong passwords don't use dictionary words or numbers in sequence.
- Don't base your password on your personal life or the service which it accesses.
- *xkcd.com/936/*has a great, humorous breakdown.

Unique Passwords

- Each service should have its own password, which in no way resembles other or old passwords.
- Using the same password for multiple services invites systemic failure.
- Reusing a password by changing one character is like not changing the password at all.

Safe Passwords

- Store your passwords someplace safe, preferably someplace that is locked or encrypted.
- If not using a Password Manager, don't store usernames and passwords in the same place.
- Don't leave passwords in plain sight or on scratch paper near the computer.
- Don't share passwords.

LUTHER COLLEGE
Information Technology Services