Information Technology Services
Information Security Office

ITS Information Security Office Educational Awareness

Topic: Password Strength

Introduction

- Password strength is a measurement of the effectiveness of a password as an authentication credential.
- The strength of any password depends on the length, complexity, and randomness.

Benefits of a Strong Password

- A strong password is the first line of defense in protecting our computer, data and online accounts.
- Advancing technology continues to make weak password easier to crack.
- A strong password makes brute force and guessing of password more difficult.

How Password are Stolen

- **Guessing**: Programs designed to automate the guessing of passwords have been developed are widely used to guess password. They often use personal information found online such as birth dates, names of friend or significant other, pet names or license plate numbers as a starting point. These programs can also search for words spelled backwards.

How Password are Stolen Continued

- **Dictionary-based attacks**: Programs and software also exist that run every word in a dictionary or word list against a user name in hopes of finding a perfect match.
- **Brute Force attacks**: By trying every conceivable combination of key strokes in tandem with a user name, brute force attacks often discover the correct password.

How Password are Stolen Continued

- **Phishing**: Phishing scams usually try to persuade you with an urgent IM or e-mail message designed to alarm or excite you into responding. These messages often appear to be from a friend, bank or other legitimate source directing you to phony Web sites designed to trick you into providing personal information, such as your user name and password.

  Note: Kennesaw State University Information Technology Services will never ask for your password via email.

How Password are Stolen Continued

- **Shoulder surfing**: Passwords are not always stolen online. An individual who is lurking around in a computer lab, cybercafé or library may be there for the express purpose of watching you enter your user name and password into a computer.

How to Create a Strong Password

- Use BOTH upper- and lower-case letters.
- Place numbers and punctuation marks randomly in your password.
- Make your password long and complex, so it is hard to crack. Between 8 to 20 characters long is recommended.
- Use one or more of these special characters: ! @ # $ % * ( ) - + = , < > : : “ ‘

How to Create a Strong Password Continued

- To help you easily remember your password, consider using a phrase or a song title as a password. For example, “Somewhere Over the Rainbow” becomes “Sw0tR8nBO” or “Smells Like Teen Spirit” becomes “sMll10nspT.”
- Make your password easy to type quickly. This will make it harder for someone looking over your shoulder to steal it.

How to Keep Password Safe

- Whenever possible, create different passwords for different accounts and applications. That way, if one account is breached, your other accounts won’t be put at risk too.
- Change your passwords regularly, about every six months.
- Never share your password with anyone else.

How to Keep Password Safe Continued

- Never enable the “Save Password” option, even if prompted to do so. Pre-saved passwords make it easy for anyone else using your computer to access your accounts.
- Never walk away from a shared computer without logging off. This will ensure no other users can access your accounts.
- Don’t use sample passwords given on different Web sites, including this one.

Conclusion

When creating a password always have in mind that a strong password provides better security to your data, computer and online accounts. The strength and management of your password combine to provide a defense against unauthorized access to your information.