PASSWORD

MANAGEMENT

Discussion Topics

- Brief History of Passwords

- How Passwords Work

- Choosing a Password

- Password Safety

- Password Manager Features

- Comparison of Password Managers

- Demonstration of KeePass

- Final Thoughts – The Future of Passwords

What's a Password?

A password, sometimes called a passcode, is a memorized secret, typically a string of characters, usually used to confirm the identity of a user.

Nuggets of Password History

- First used in ancient times

- Examples found in the Bible – Shibboleth

- Julius Caesar used substitution ciphers

- Ali Baba and the Forty Thieves – Open Sesame

- Who is Fernando Corbato? Why is he important in Password History?

Fernando Corbato

Worked at MIT in 1960

All workers shared on main frame computer

Invented password algorithm to keep individual files private from other workers

Called the "Godfather of the Modern Computer Password"

All modern secure computer systems store users' passwords in an encrypted format. Whenever a user logs in, the password entered is encrypted initially, then compared to the stored encryption of the password associated with the user's login name. A match succeeds and a mismatch fails. Isn't that simple?

Password Problems

- Site might not use strong encryption
- Password might be exposed prior to encryption
- System support techs might not be trustworthy
- Could be logging into the wrong site
- Different sites have different rules

Tips For Choosing A Password

- Use stronger passwords for important things

- Longer passwords are usually stronger

- Include uppercase, numbers, special characters, etc.

- Don't use obvious personal information

- Don't reuse passwords

- Decide when to change your passwords

THREE

RULES

TO KEEP

YOUR

PASSWORDS

SAFE

PASSWORDS are like UNDERWEAR

1. Change them regularly

2. Don't leave them on your desk

3. Don't loan them to anyone

Storing Your Passwords

- Post It Notes
- Loose Leaf Notebook
- Rolodex File
- Spread Sheet
- Notepad File

All of these methods could be effective if

1) you don't have many passwords

2) you only use one computer

3) you don't mind spending lots of time on passwords

USE A PASSWORD MANAGER!

Password Manager

- A software application that is used to store and manage passwords
- Many types of password managers

    1) encryption method

    2) storage method

    3) password generation method

    4) other features

- Several types of password managers

    1) browser

    2) cloud

    3) desktop

    4) portable

Browser Password Managers

PROS

- Most major browsers have the feature
- Easy to use
- Passwords synced on all devices
- Service is Free

CONS

- May not be as safe
- No cross-browser synchronization
- Limited security features
- Much more risk

Standalone Password Managers

PROS

- Multi-purpose use

- Better Security

- Passwords synced on most devices

- Many have helpful add-ons

CONS

- Not always free

- Only as safe as the company

- Single point of failure

Password Manager Features

- Encryption – don't believe all the advertising
- Ease of Use

In my opinion, these are the only real important items

1- if anyone can read the password file, why use one?

2- if the program isn't easy to use, you will end up not using it.

Decide for yourself what other features are important to you.

Other Features

- Multi-Platform Support

- Password Generator

- Online Storage

- Recovery Options

- Device Synchronization

- Save and Autofill

- Item Storage

Free vs. Paid

- I'm not going to compare Password Managers. An internet search will yield thousands of sites that can do it better than me.

- Many paid managers have a limited free users option.

- Some paid managers have a test period.

- Some free managers make money by selling your info – e-mail, name, address, phone, etc.

Research and Test

KeyPass Demonstration

Why a KeePass Demo?

1) Has most of the major password features

2) Only one installed on my computer

3) I've used for more than 10 years

KeePass Features

- Totally Free – just download and install
- Open Source – code can be downloaded and tested by anyone
- Strong Security – several algorithms supported
- Secure Clipboard – clears after set time
- Strong Password Generator – defined by user
- Supports Plug-ins – increases functionality
- [Many More](#)

Ready for a demonstration?

Upcoming Topics

- February 16 – How Web Browsers Work

- February 23- Web Browser Extensions

- March – About Android (4 weeks)

If you'd rather have different topics, let me know and I'll make a change.

Download Presentations   KeePass Tutorial
toxitman.com

THANKS FOR LISTENING ☺