Cybersecurity for Quilt Guilds

Dr. Linda F. Wilson

Professor of Computer Science

Texas Lutheran University

TLU
TEXAS LUTHERAN UNIVERSITY

Outline

- Introduction
- Password Security
- Online Privacy in General
- Facebook and Social Media
- Web Sites
- Sharing Documents and Information
- ADA Compliance
- Spam Email & Phishing
- Other Suggestions
- Q & A

Introduction

- Hackers
  - o Are everywhere
  - o Use automated tools

Introduction

- Hackers
  - o Are everywhere
  - o Use automated tools
- Constant battle: Good vs. Evil

Useful Tactic

- Make things hard enough that attacker will go bother someone else
- Analogy: Home with locks, security system, cameras

Password Security

- Vital for all of your accounts – email, Facebook, bank, etc.

- Password security problems cause numerous cybersecurity issues!

Poor Password Practices

- Using a short, simple, easy-to-guess password
  - password, 1234, **quilting**, **Jenny**
- Using the same password for multiple accounts
- Sharing your password with others
- Writing down your password

Good Password Practices

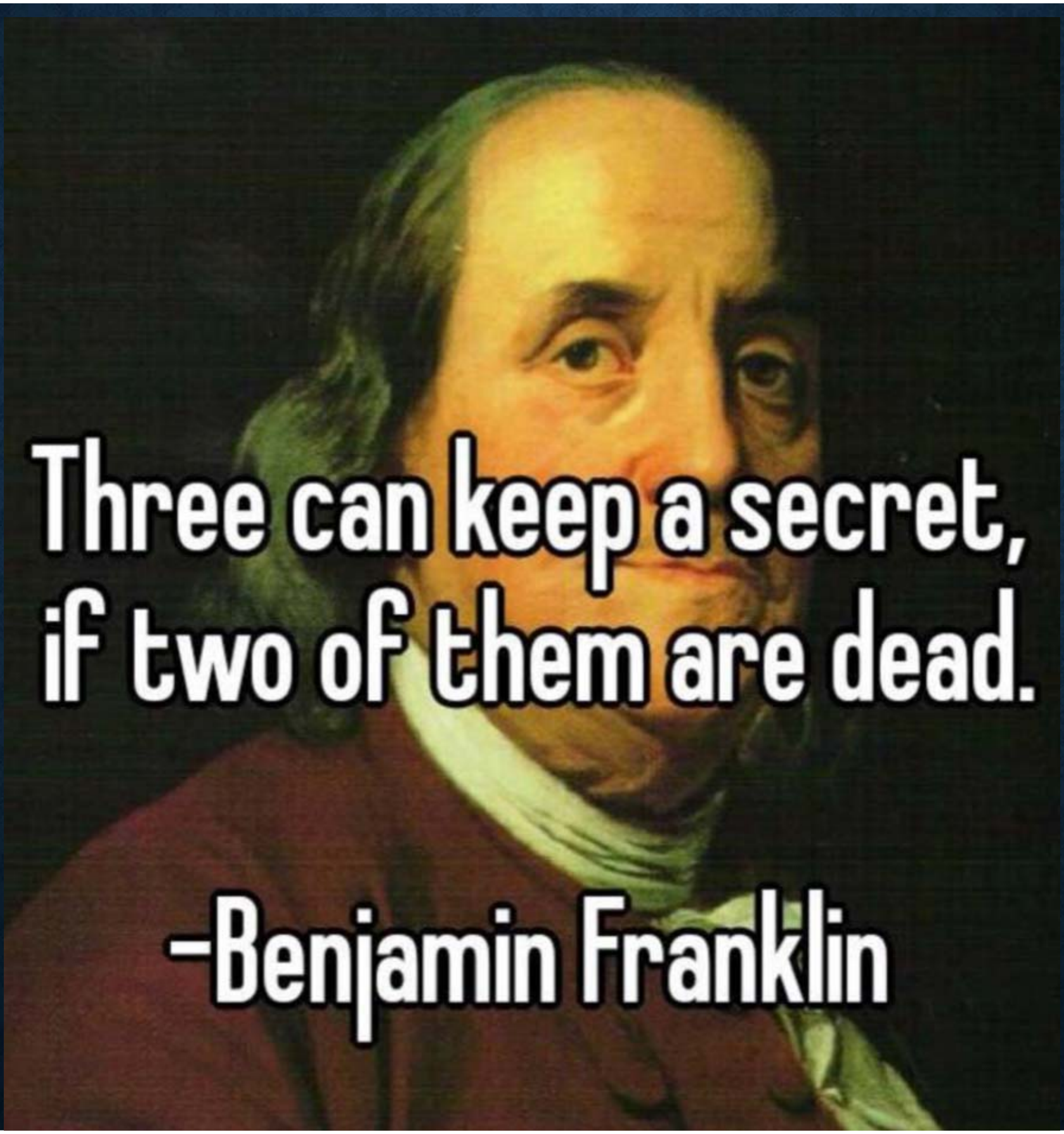
- Using a long, complicated, hard-to-guess password
  - **Qltz4evrM0R!!**
  - **QuiltsForeverMore!!**

Good Password Practices

- Using a long, complicated, hard-to-guess password
  - **`Qltz4evrM0R!!1776`**
- Enabling 2-factor / multifactor authentication (MFA)
  - Get text or email with a random **code** to be entered
- Using a different password for each account

Good Password Practices

- Using password management software
  - iOS has built-in password manager
  - Norton Utilities has password manager
- Keeping passwords secret



Three can keep a secret,
if two of them are dead.

-Benjamin Franklin

Key Point

- Your password is the key to everything in your account!

Online Behavior in General

- Don't assume any privacy for anything you post online
  - Social media accounts frequently are compromised due to weak passwords
    - Maybe your password is secure, but what about your friend who sees your posts?
  - Despite permissions, people can find a way to share posts and pictures
  - Search engines can find all kinds of information

Facebook Groups

- Public Groups
- Private Groups

Facebook Groups

- Public Groups
- Private Groups
- Warning: Facebook makes its money by harvesting data from its users

Facebook Groups

- **Public** Groups
  - Anyone can find public groups
  - Content is not limited to members of the group
  - The member list is public and visible to anyone on Facebook
  - Content can be seen by **anyone**, even if they don't have a Facebook account

Facebook Groups

- **Private** Groups
  - Only members have access to posts inside the group
  - Only members can see the list of members
  - Anyone on Facebook can see who the administrators and moderators are

Facebook Groups

- **Private** Groups
  - Only members have access to posts inside the group
  - Only members can see the list of members
  - Anyone on Facebook can see who the administrators and moderators are
  - BUT, if a member's Facebook password has been compromised ….

Facebook Groups

- Administrator
  - Has complete control of the group, including managing group settings, naming administrators & moderators, plus all capabilities of a moderator
- Moderator
  - Can approve or deny membership, approve or deny posts, remove posts, remove and ban people from group

Web Site Security

- Have VERY strong password for administrator account
  - Have no more than 2 administrators
- Require username and password for information on your site that needs to be protected

Web Site Security

- Have VERY strong password for administrator account
  - Have no more than 2 administrators, each with own account
- Require username and password for information on your site that needs to be protected
  - Require long, complicated passwords

Web Site Security

- Have VERY strong password for administrator account
  - Have no more than 2 administrators, each with own account
- Require username and password for information on your site that needs to be protected
  - Require long, complicated passwords
  - Ideal: Require that passwords be changed after certain period of time

Sharing Documents

- Send by email
  - Everyone (usually) gets their own copy of the document
  - Nobody sees if someone make an update to their copy

Sharing Documents

- Post on Google Docs (docs.google.com) or Google Drive and then share link
  - Great for everyone having access to **same version** of document
  - Can limit access to list of email addresses OR anyone with the link
  - Can limit to read-only access OR allow others to edit

Sharing Documents

- Post on Google Docs (docs.google.com) or Google Drive and then share link
    - If link is only requirement for access:
        - More secure if link is shared at guild meeting or by email
        - Could also share link via Private Facebook group or secure web page

Sharing Documents

- Post on web site
    - Be aware that documents can be "harvested" by hackers' automated tools
    - Better if in secure section of web site

Sharing Personal Information

- The more you share, the easier you make it for hackers!
  - If you share birthday information, **never** put the year / age
  - If you share pictures, be aware that others might copy them

- Disclaimer: I am not an attorney and cannot advise about privacy laws!

Sharing Financial Information

- Make the financial documents **password-protected**, and then share them carefully
  - Via email
  - Via Google Docs to restricted list of users
  - Via Google Docs or Private Facebook Group or restricted area of web site

Heads Up

- SMS Text Messages are **not** secure
- iOS iMessages are generally secure
- FB Messenger messages generally are **not** secure
  - Can use "Secret Conversation" in Messenger but most people are not aware of it

ADA Compliance

- Not my area of expertise
- For documents such as Word and PowerPoint, there is an accessibility checker
  - Menu: Review → Check Accessibility

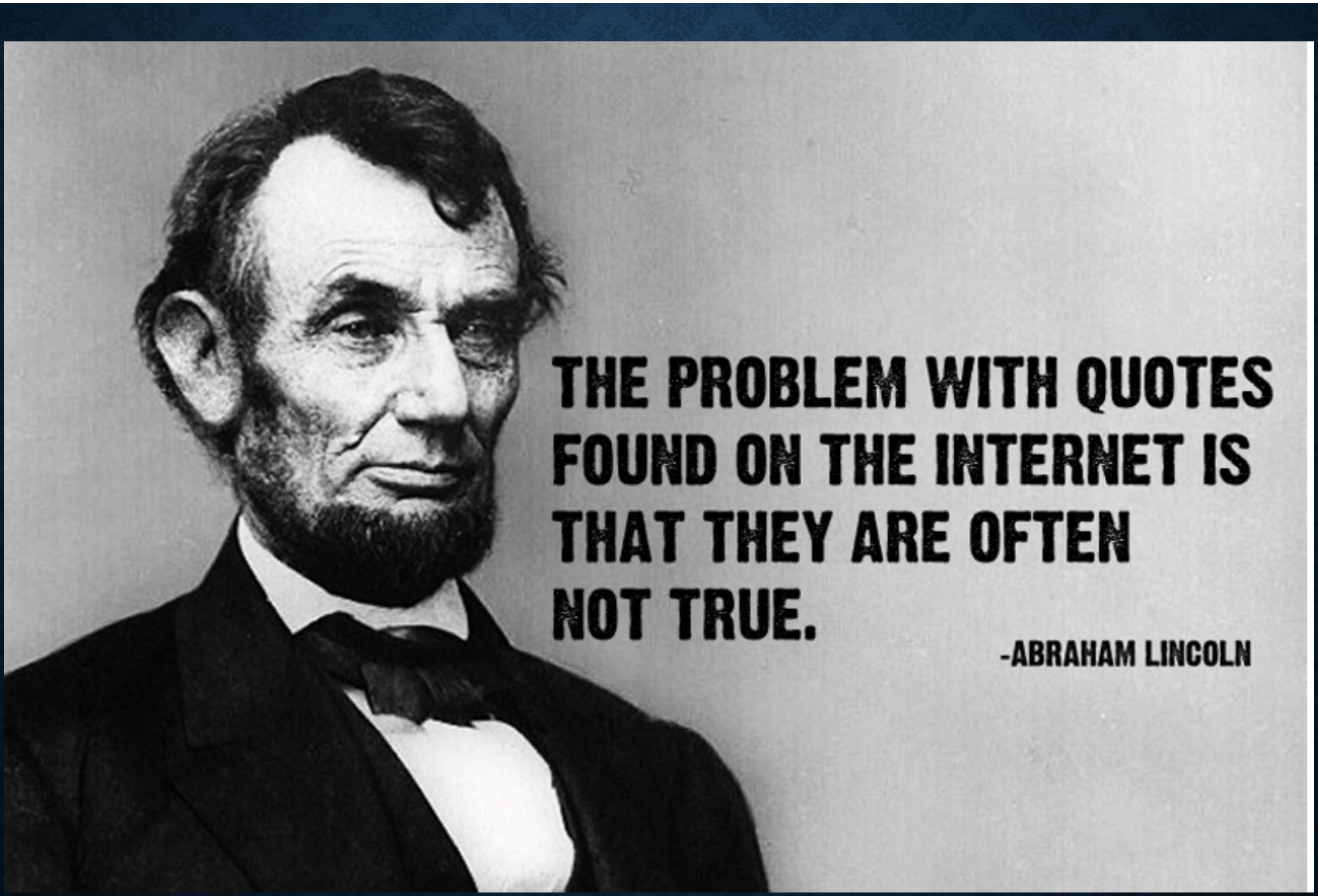
Spam Email and Phishing

- Hackers use automated tools to collect email addresses
- Tip for posting email address:

nbaqgpresident AT gmail DOT com

Other Suggestions

- If you get spam/phishing email:
  - Report it to your email provider
  - Report it to the company that was faked / spoofed
- Work with your web provider to make sure appropriate security measures are in place
  - Ask them what security features are being used for your site, and if there is anything else they can do



THE PROBLEM WITH QUOTES FOUND ON THE INTERNET IS THAT THEY ARE OFTEN NOT TRUE.

-ABRAHAM LINCOLN

Questions & Answers