The Top 10
IT Security
DO'S and DON'TS
For Churches

1. DO take security seriously

Why should I care about IT security?

- Financial consequences
- Compromise of personal or confidential information
- Loss of valuable organizational information or intellectual property
- Loss of staff and congregation trust, loss of reputation, embarrassment, bad publicity, media coverage

- 90/10 Rule
  - 10% of security safeguards rely on technology
  - 90% of security safeguards rely on the user

Why should I care about IT security?

- The average cost per record of a data breach in 2016 was $158
- The average amount paid by ransomware victims more than doubled in 2016
- Microsoft cyber attacks: 10M login attempts daily
- Attacks are becoming more frequent, more sophisticated, and more expensive

What can hackers do with my computer?

- Record keystrokes and steal passwords
- Send spam and phishing emails
- Harvest and sell email addresses and passwords
- Access sensitive information
- Infect other systems
- Illegally distribute music, movies, software, and inappropriate content
- Slow down your whole network by generating large volumes of traffic

2. DON’T get tricked into sharing confidential info

Threat: Social Engineering

- Social Engineering: when scammers use social interaction to steal data or gain unauthorized access
- Strategies:
  - Find and use information
  - Exploit familiarity
  - Exploit sympathy
  - Exploit desire to be helpful
- Results of our secret email test

WATCH HERE: https://youtu.be/lc7scxvKQOo

Threat: Social Engineering

- Phishing- Email that looks like it came from someone trusted, who is requesting information
  - Three quarters of social engineering attacks are phishing attacks
  - Spear phishing- targeted attack personalized to you
  - CEO Fraud- Email from the CEO/Lead Pastor requesting money, etc
- Vishing- A phishing phone call
  - Call pretending to be your IT vendor requesting login information or access
  - Pretending to be from another campus or from a familiar vendor
- Tailgating- Gaining access into a secure area by following behind someone
  - Don’t neglect physical security

Best Practices: Social Engineering

- Train your staff!
- If a hacker called an employee at your church pretending to be the IT department, how would they respond?
- Stopping these attacks depends on your staff
- No amount of technical IT security can take the place of common sense
- Training should be ongoing, like fire drills

3. DO use complex, unique passwords

Best Practices: Passwords

- Passwords won't protect you if you don't protect them
- Use unique passwords for each website
- Use a password manager

  Recommended: 1password, LastPass, DashLane

- Characteristics of strong passwords:
  - Contain a mixture of upper and lower case letters, numbers, and symbols
  - At least 8 characters in length
  - Easy to remember, difficult to guess

Most Common Passwords of 2016

- 123456
- password
- 12345678
- qwerty
- zxcvbnm
- 777777
- football
- Sunshine
- 1q2w3e
- 654321
- baseball
- welcome
- 1234567890
- abc123
- 111111
- 1qaz2wsx
- dragon
- Password1
- master
- monkey
- letmein
- login
- princess
- qwertyuiop
- loveme
- passw0rd
- starwars

4. DON’T leave sensitive information around the office

Put Things Away

- Don't leave printouts containing private information on your desk
- Lock them in a drawer or shred them
- It's very easy for a visitor to glance down at your desk and see sensitive documents
- Types of documents to protect include
  - Resumes
  - Financial documents
  - Personal identifying information (DOB, SSN, address, etc.)
  - Counseling/pastoral notes
  - Benevolence notes
  - Employee records
  - Passwords!

5. DO lock your devices

Don’t Leave Your Front Door Open

- Always lock your devices when you're not using them
  - Set them to auto-lock when not being used
- Devices are easily stolen from offices, cars, and homes
- Our phones offer direct access to our personal information, privacy, and financial accounts
- Not to mention access to work files and emails
- For most of us, our first reaction when we lose our wallet is I have to cancel my credits cards, get a new license, etc.

6. DON’T send sensitive info via email, text, or IM

Text, Email, and IM

- Never assume these types of communication are private
- Only use trusted, secure web pages when entering personal or sensitive information
- Don't log in to web sites or online applications unless the login page is secure
  - Look for https (not http) in the URL to indicate that there is a secure connection
- Be especially careful about what you do over wireless
- Information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept
  - Most public access wireless is unencrypted

7. DO be suspicious of emails, links, & attachments

Think First

- Don’t let curiosity get the best of you!
- If you aren’t expecting it, don’t click on it
- Use healthy skepticism
  - Is there really a Nigerian prince who will make me rich?
  - Would our pastor really ask me to wire money?
- Always delete suspicious emails and links
- Opening these emails and links can compromise your computer and create unwanted problems without your knowledge

Threat: Ransomware

- Ransomware allows an attacker to kidnap your data by encrypting it
- Your data is held hostage unless you pay for the encryption key
- Attacks come through e-mail attachments, infected websites, etc.
- Paying the ransom encourages more attacks

Best Practices: Ransomware

- Be cautious when opening attachments or clicking links
- Keep anti-virus updated
- Report suspicious activity ASAP
- If you suspect ransomware, unplug your computer ASAP
- BACK UP YOUR DATA

8. DON’T install unauthorized programs

Installing Applications

- Free software - if something looks too good to be true, it probably is
- Malicious applications often pose as legitimate programs, like games, tools, or other software
  - They can harbor behind-the-scenes viruses or open a "back door" giving others access to your devices without your knowledge
  - They aim to fool you into infecting your own computer or network
- If you think an application will be useful, contact IT to look into it before installing

9. DO stay alert and report suspicious activity

See It, Say It

- Always report any suspicious activity
- Part of our job is to make sure your data isn't lost or stolen
- If something goes wrong, the faster we know about it, the faster we can take action

10. DON’T forget to secure your personal devices

Stay Secure at Home

- Your personal information is sought after and should be secured
- Most of us use personal devices to access work files, emails, etc.
- Remember PAUL
  - Password
  - Anti-virus
  - Update
  - Lock

Sources:

- http://www.social-engineer.org/
- http://its.ucsc.edu/security/
- https://www.sophos.com/en-us/security-news-trends/
- https://www.knowbe4.com/
- http://ministrytech.com/category/internet-security/
- http://www.networkworld.com/article/3160101/security/top-25-worst-of-the-worst-most-common-passwords-used-in-2016.html

- Ready to test your savvy? Take this quiz: https://www.sonicwall.com/phishing