Congregation Information Security Awareness

Disclaimer: This information is not intended to provide security, legal, financial or other professional advice. Any institution or congregation should seek the services of a competent professional for such advice.

Evangelical Lutheran Church in America
God's work. Our hands.

Our Goal:

Stress common sense and emphasize caution when handling constituent information

Awareness

Individuals are aware of how to properly protect information and the risks to the confidentiality, integrity, and availability of information.

Avoid

Avoid-common mistakes and realize the consequences of failure to protect.

Responsibility

How to protect sensitive information and what action to take when there are valid reasons for suspecting theft, damage, or misuse of information to safeguard our organizations reputation.

Benefits

Protecting the church and investing in its future.

What is Information classification?

Information Classification

- Categorizing information according to its nature (confidential, restricted, public) to properly handle and secure.
- The sensitivity of each piece of information must be identified, or 'classified'.

Types of Information classification

- **Public** – published without restrictions.
- **Restricted** – shared at owner's discretion.
- **Confidential – Personally Identifiable Information (PII)** Never distributed outside the of the congregation.

Public Information

Public information consists of documentation, logos, reports and electronic media that is meant for public consumption.

Some examples include:

- Publications on the congregation website
- News Releases
- Official communication from the church leadership
- Job postings
- Church Bulletins

Diligence must be exercised (and sometimes approval) when deciding what is allowed to be publicly available/posted/etc.

Restricted Information

Restricted Information is related to reports and electronic media that is not to be released to the general public. This information may be used to harm the congregation, synod or its constituents, but unlike confidential information (Next slide) it does not reveal individualized information about employees, donors and customers.

Some examples include:

- System passwords
- Budgets
- Weekly collection amounts

Confidential Information

Confidential: **Personally Identifiable Information (PII)**

PII is never given to anyone outside the of the congregation*

PII examples include, but are not limited to:

- Name and address
- Birth dates
- Social Security numbers
- Credit card information
- Passport / driver's license
- Financial information / donation history
- Bank account and routing numbers
- Financial information

Breaches of PII expose the congregation to liability

*With rare exceptions, like congregation's payroll vendor

Where Confidential Information Resides?

Be aware of cyber crimes...

Computer crime is one of the fastest-growing types of illegal activity, both in the U.S. and internationally.* While the Internet links people together with email and social media, it also provides endless opportunity to criminals seeking to exploit the vulnerabilities of others. Some examples are:

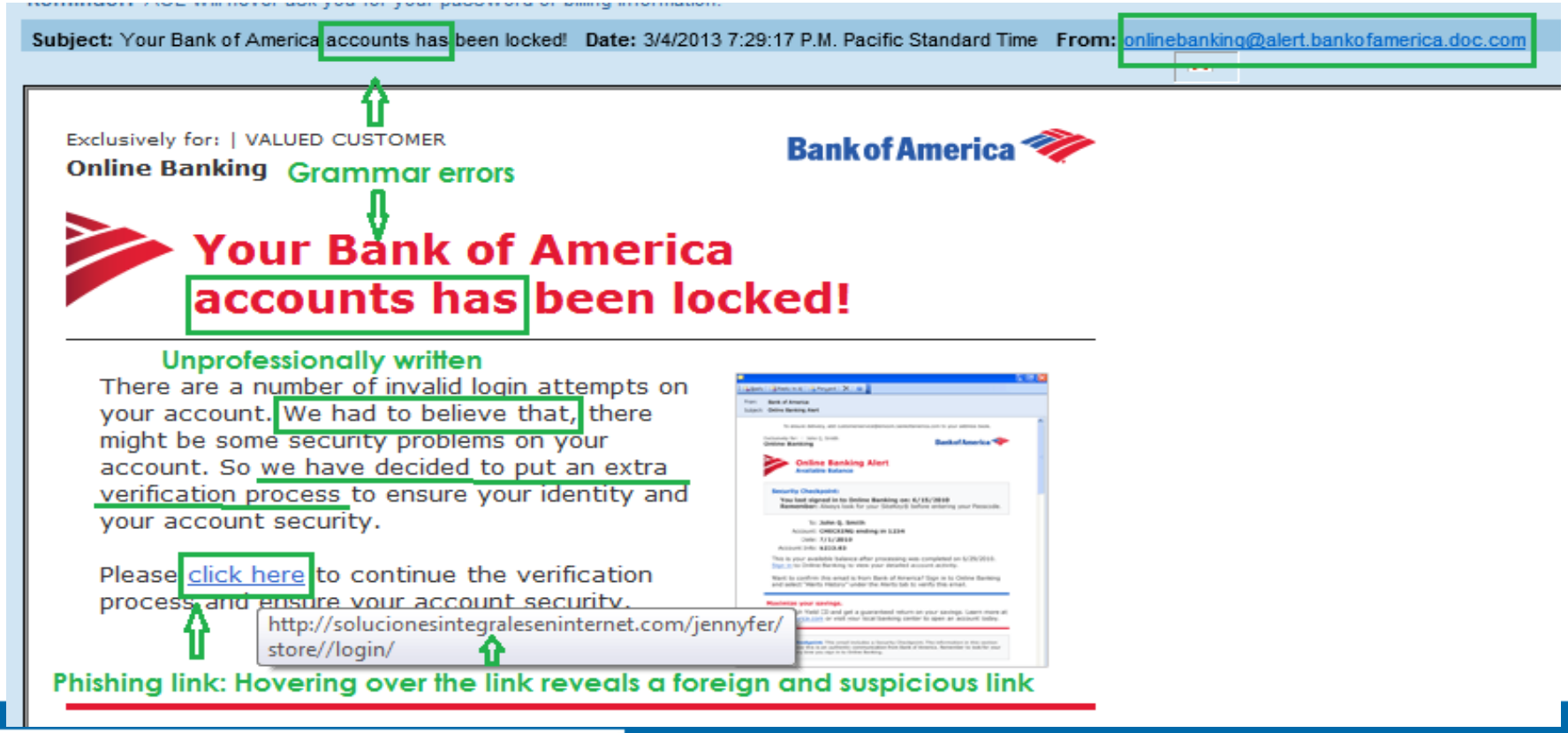
- Phishing
- Hacking
- Cyber Stalking
- Social Engineering

*http://www.cnbc.com/2016/09/28/the-2016-trends-in-cybercrime-that-you-need-to-know-about.html

Phishing

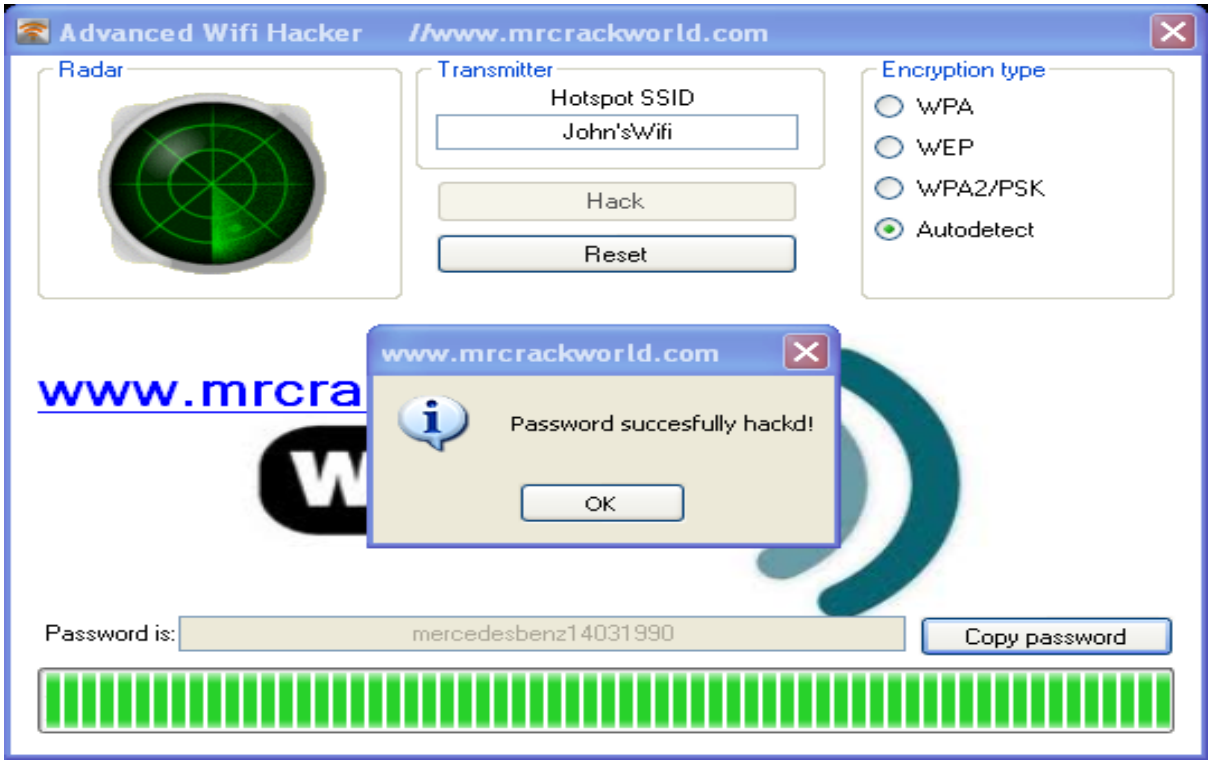
Phishing is the practice of sending fraudulent emails in an attempt to trick the recipient, usually for the purpose of obtaining information.

This information can be used to breach a computer system, extort money, or create disruption.



Hacking

Hacking is similar to digital trespassing. Hackers infiltrate online networks to illegally download confidential information, manipulate functions and, in some cases, steal identities that can be used to fraudulently purchase goods online.



Protecting yourself online

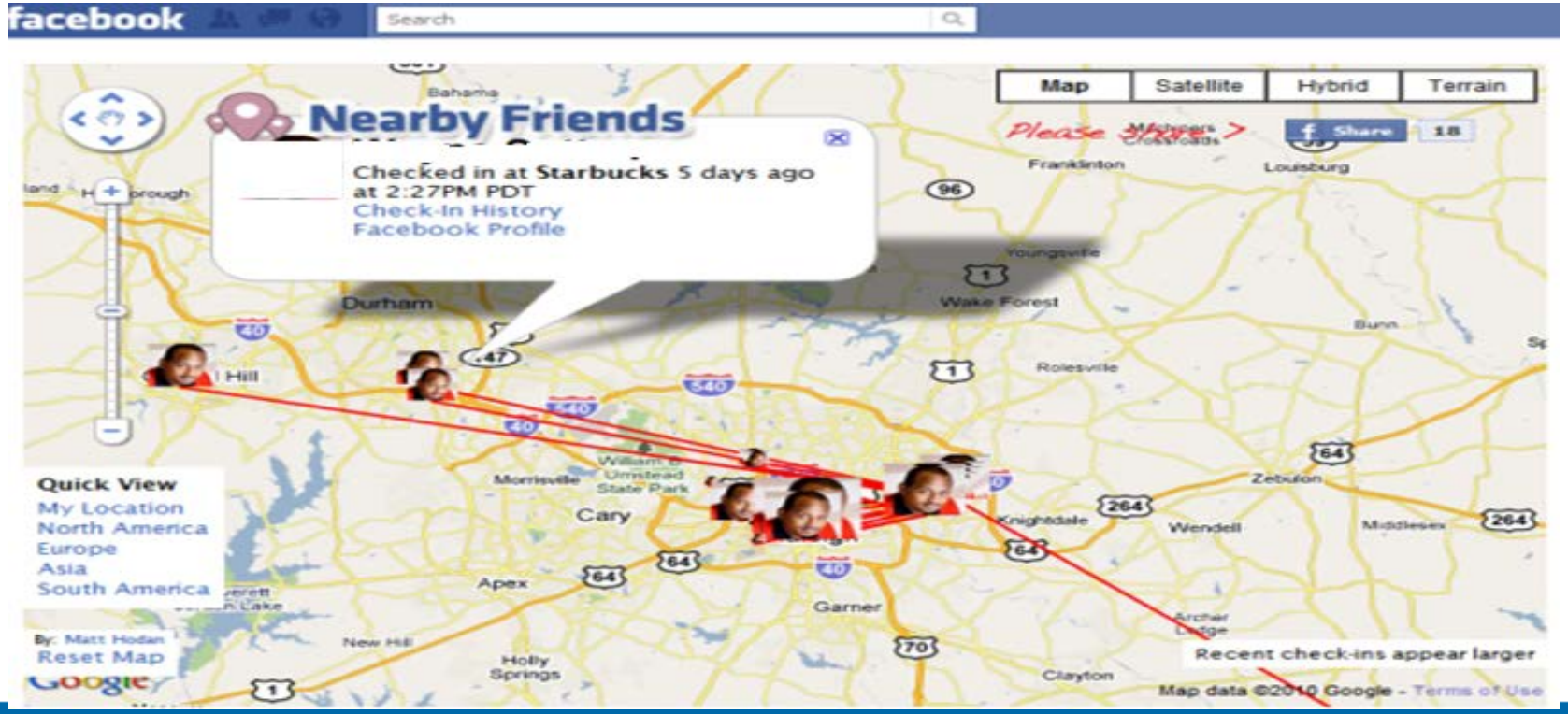
Security: We must secure our computers in the same way that we secure our property.

Safety: We must act in ways that protect us against the Internet risks.

Steps you can take		
Your Computer 1. Enable Internet firewall. 2. Install and maintain antivirus software to detect and remove viruses. 3. Review website privacy statements and avoid untrusted sites.	**Your family and co-workers** 1. Talk with your family and co-workers about online safety. 2. Set rules for Internet use. 3. Keep personal information private (e.g. passwords, files).	**Your Personal Info** 1. Be careful of what you post on the internet. 2. Know what information is publicly available about you. 3. Make sure your social media security settings are set properly.

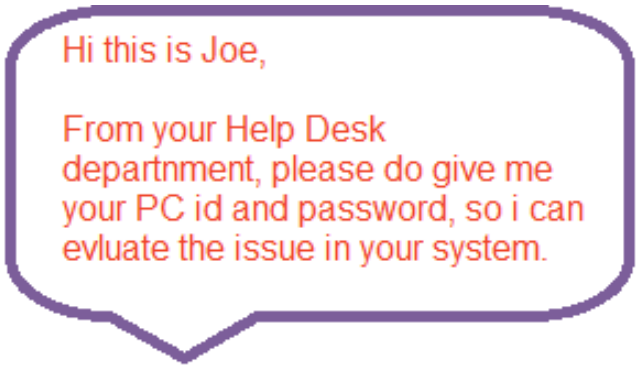
Cyber Stalking

Stalking and/or Harassment – Not all types of cyber crime involve money. Some cyber criminals use the Internet as a cover for other illegal behaviors like stalking, harassment and in other cases, bullying.



Social Engineering

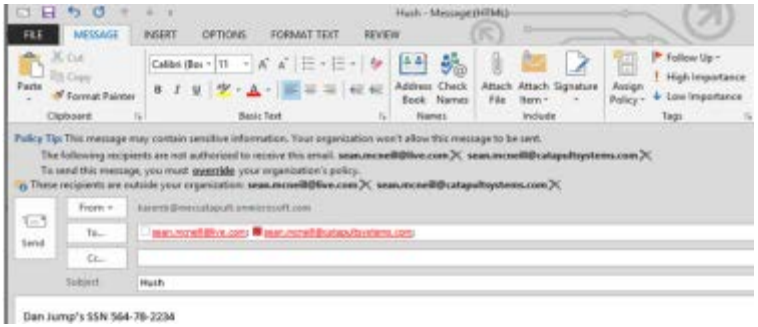
Practice of deceiving someone, either in person, over the phone, or using a computer, with the express intent of compromising security or obtaining information to do harm.



The human is the weakest link in the security of information. What are common mistakes we should avoid?

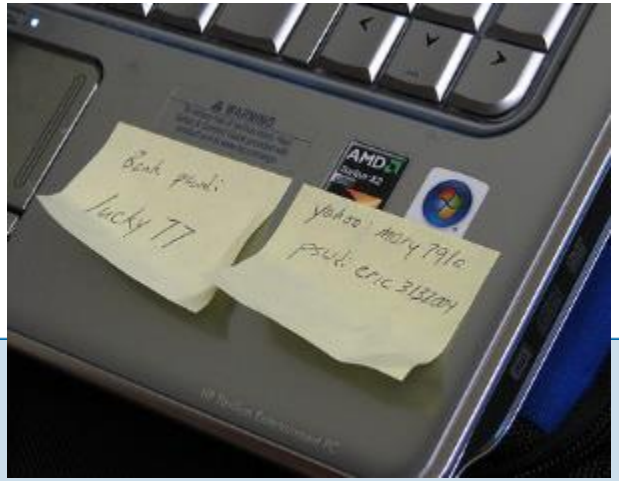
Storing or downloading confidential information on mobile devices (e.g. laptops, flash drives, CD's) or file sharing sites like Google Docs, Dropbox etc.

Avoid messages and attachments containing confidential information in outbound emails



Paper disposal: 1 in 3 people admit they throw away documents containing PII without properly shredding them

Passwords on Post-it notes or Monitors



What is at stake?

Compromise of credentials

Yahoo experiences biggest data breach in history: 1 billion affected

BY NARINDER PURBA POSTED 15 DEC 2016 - 11:00AM

NEWS

Financial Loss

Target Expects $148 Million Loss from Data Breach

Loss of Job

9 data breaches that cost someone their job

What is at stake?

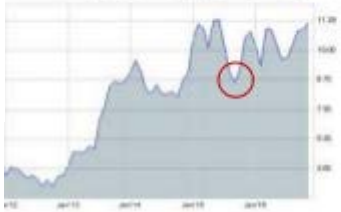
Lawsuits/Fines

LinkedIn Settles Data Breach Lawsuit

The social network has agreed to pay a total of $1.25 million to breach victims in the U.S. who paid a fee to LinkedIn for a premium subscription between March 15, 2006, and June 7, 2012, according to the settlement. Each individual will receive a share of up to $50. "That amount is at least equal to, and likely surpasses, the amount that the individual LinkedIn subscribers could expect to receive at trial," according to the settlement, which was submitted in the U.S. District Court for the Northern District of California on Aug. 15 for preliminary approval.

Loss of trust and ruined reputation

Wendy's stock were down 1.14% to $9.52 in midday trade after the company announced that it had learned more about recent "malicious cyber activity" at various locations in June.



A leading research institute (Ponemon) revealed that data breaches were up there with poor customer service and environmental disasters for impacting brand reputation.

How to protect PII on personal devices?

When using your personal device to access PII

- Use “hard to guess” passwords
- Never share passwords with anyone
- Do not leave information displayed on screen
- Install and run anti-virus software
- Never download or save confidential information on your mobile device
- When unattended, keep devices secure and lock your screen

- Consider public computers unsafe
- Turn off connections not-in-use
- Do not download unauthorized software
- Don’t use unauthorized file sharing software / websites
- Keep your personal and work information separated
- Avoid free public Wi-Fi

How to protect PII on printed materials?

Printed reports, letters, forms and documents stored in physical archives.

- Ensure that all printouts containing PII are stored in a locked file cabinet when not in use.
- Physical documents should be shredded when no longer needed.
- Do not print anything containing PII unless it is absolutely necessary.
- Ensure confidential documents needed for retention are archived in a timely manner.

- Treat paper the way you hope credit card companies are treating your statements.
- While printing confidential information make sure it's to a printer in a secure location.
- Ensure recipients of paper reports understand the applicable sensitivity of the report.
- Scan paper documents into a PDF or other electronic format.

How to protect PII when sharing information?

When sharing PII via Email or the Internet

- While copying or forwarding emails make sure PII is not included.
- Never send anything by fax or e-mail that you wouldn't put on the back of a postcard
- Control is lost once email is sent
- Make sure confidential documents are password protected
- Think before you use social media and follow acceptable usage guidelines
- If you provide individuals with remote access to your system, don't leave your computer unattended and carefully review why they need the access and how long will they need it for.
- Do not disclose any confidential information on public web sites
- Encrypt email if you need to send something with confidential/restricted information

It takes all of us to be proactive and committed towards making our organization a safe and secure place for everyone.

Exercising diligence when handling confidential or restricted information is a key to avoiding exposure.

Always be cautious when using the internet.