CYBERSECURITY:

Solutions for Not-For-Profit organizations

Not-For-Profit Training Conference
May 3, 2019
Cindy Gross, CPA, CISA, C|EH

BROWNEDWARDS
certified public accountants

Learning Objectives

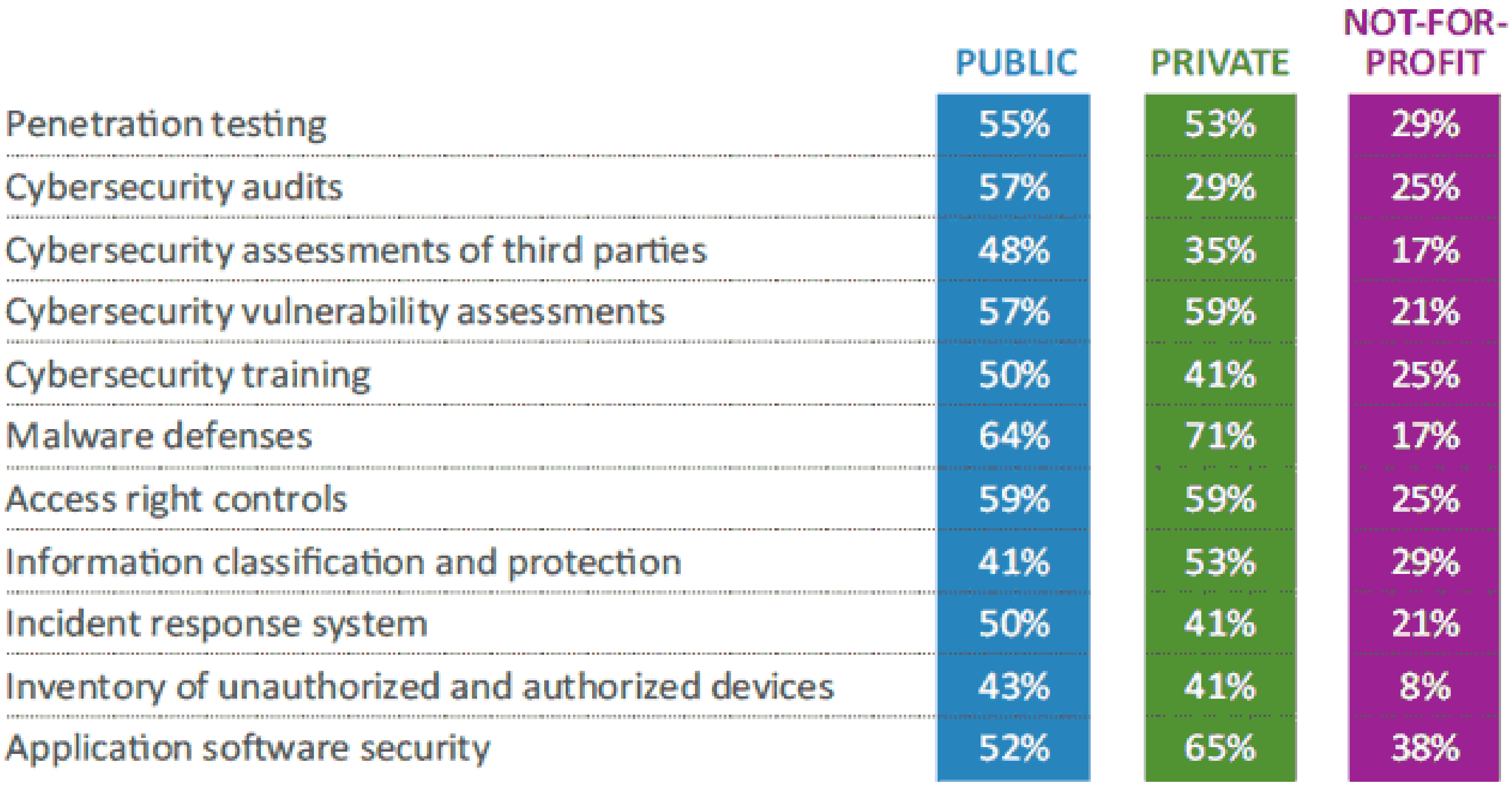
- Nonprofit cyber statistics
- When cybersecurity efforts really matter
- Common threats
- Low-cost solutions and best practices

Statistics

- 70% of nonprofits have not had a vulnerability assessment performed
- 69% of nonprofits do not have a cybersecurity response plan
- Sixth most targeted industry
- Over a 4 year period, the average cost per breach for a nonprofit was $84,000

Statistics

What methods have been employed to address cybersecurity risks?



	PUBLIC	PRIVATE	NOT-FOR-PROFIT
Penetration testing	55%	53%	29%
Cybersecurity audits	57%	29%	25%
Cybersecurity assessments of third parties	48%	35%	17%
Cybersecurity vulnerability assessments	57%	59%	21%
Cybersecurity training	50%	41%	25%
Malware defenses	64%	71%	17%
Access right controls	59%	59%	25%
Information classification and protection	41%	53%	29%
Incident response system	50%	41%	21%
Inventory of unauthorized and authorized devices	43%	41%	8%
Application software security	52%	65%	38%

When Cybersecurity Matters

If your organization engages in any of the three listed activities, it's time to get serious about cybersecurity risks.

- Conduct e-commerce on a website
- Store and transfer personally identifiable information (PII)
- Collect information on preferences and habits of donors, patrons, or newsletter subscribers

Common Threats

The causes of breaches are typically thought of as malicious, but they can also be unintentional. Common cyber threats include:

1. **Inside attackers**
2. **Outside attackers**
3. **Viruses and malware**
4. **Employee accident**
5. **Non-malicious system or coding errors**
6. **Trusted third-party vulnerabilities**

Low-Cost, High-Priority Solutions

Entity Level

1. **Assess your risk.**
   - Risk assessments can be conducted within the organization but many use outside specialists
   - Cyber assessments should be updated and reassessed as often as possible
2. **Upgrade computers and software.**
   - Make sure computers and network operating systems are always updated.
3. **Train and inform employees and volunteers.**
   - Make sure everyone is on the same page and alert to these kinds of threats.

Low-Cost, High-Priority Solutions

Entity Level

4. **Invest in reputable nonprofit technology.**
   - Consider using an email provider to send email blasts and fundraising appeals
   - Explore purchasing a CRM system

There are important data security risks to consider when storing data in the cloud.

Low-Cost, High-Priority Solutions

Entity Level

- Begin with data classification.
  - Identify the data processed or stored in the cloud.
  - Classify the information in regards to sensitivity.
  - Define the rules for storing, transmitting, archiving, transporting and destroying data.
- Find a provider that can handle restrictions on the physical location of data.
- Methods to meet your data protection requirements:
  - File system access control lists
  - Encryption with a mixture of public and private keys
  - Transport level encryption

BROWNEDWARDS
certified public accountants

Low-Cost, High-Priority Solutions

Entity Level

5. **Use a reputable online payment processor.**
   - A majority of nonprofits use PayPal, but give donors at least one other option.
   - Be aware of how fraudsters can process fake donations using stolen credit card numbers.

Use some of the following strategies for online payments:

Low-Cost, High-Priority Solutions

Entity Level

- Donors should have access to the card they are using.
  - Verify CVV2 code
  - Verify the address
- Verify the cardholder's identity.
  - BIN/IP address verification
  - Two-factor authentication
- Make donation form more sophisticated.
  - Require a minimum transaction amount
  - Use encryption and tokenization

Low-Cost, High-Priority Solutions

Entity Level

6. **Institute a cybersecurity breach response plan.**
   - A plan will help ensure that you can react quickly and be strategic.

To ensure your plan is effective, it should include the following four elements:

Low-Cost, High-Priority Solutions

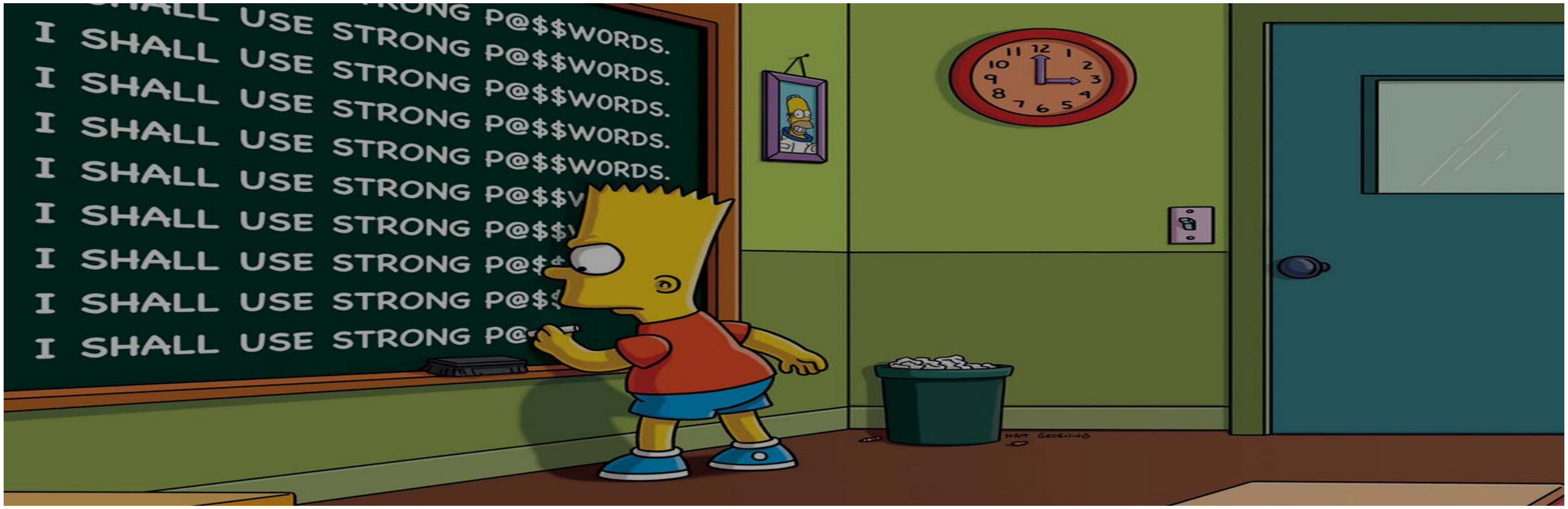
Entity Level

- It’s Tested Consistently
- It’s Detailed but Flexible
- It’s Clear About Communication
- It’s Inclusive When It Comes to Stakeholders

Low-Cost, High-Priority Solutions

Individual Level

1. **Focus on passwords.**
   - Do not have the same password for every account.
   - Consider using a password manager.
   - Mix up the types of characters you use.



Low-Cost, High-Priority Solutions

Individual Level

2. **Information stewardship.**
   - You should only have access to information required for your job position.
   - When storing sensitive information:
     - Store data in accordance with data classification policies
     - Never transmit, store, or process sensitive data on a non-sensitive system
     - Label paperwork containing PII appropriately
     - Use secure bins
     - Keep only what you need

Low-Cost, High-Priority Solutions

Individual Level

3. **Social Engineering best practices.**
   - For calls: document the situation.
   - Don’t share personal information.
   - Don’t give out computer system or network information.
   - Listen to your gut.
   - Scrutinize email addresses and the text of URLs.

BROWNEDWARDS
certified public accountants

Low-Cost, High-Priority Solutions

Individual Level

3. **Social Engineering best practices (cont'd).**
   - Protect your facility.
     - Always use your own badge
     - Never grant access for someone else using your badge
     - Challenge people who do not display badges
     - Report any suspicious activity
   - Avoid discussing sensitive operations outside work premises.
   - Be discreet when retrieving messages from smart phones.

Low-Cost, High-Priority Solutions

Individual Level

4. **Report suspicious computer problems.**
   - Methods to prevent viruses.
     - Remove software you don’t use
     - Keep internet activity relevant
     - Log out at the end of the day
     - Update your operating system, browser, and plugins
     - Only access SSL protected websites

Low-Cost, High-Priority Solutions

Individual Level

5. **Social media best practices.**
   - Be aware of what you post online.
   - Ensure you monitor privacy settings.
   - Refrain from discussing work-related matters on social media sites.

BROWNEDWARDS
certified public accountants

Low-Cost, High-Priority Solutions

Individual Level

6. **Wire transfers.**
   - Verbal communication
   - Verify changes
   - Investigate unique requests
   - Double check email addresses
   - FWD Instead of Reply
   - Be Alert

BROWNEDWARDS
certified public accountants

Low-Cost, High-Priority Solutions

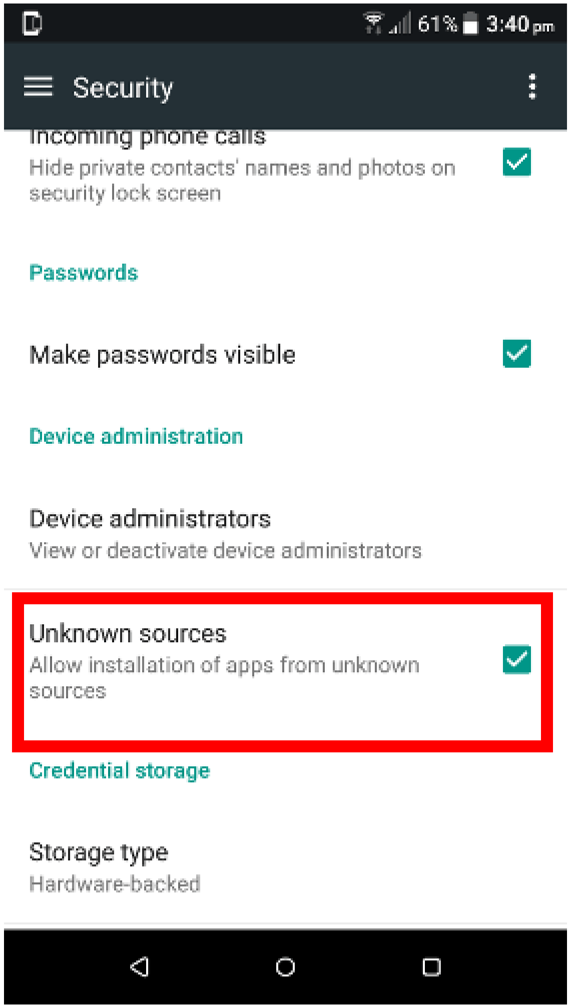
Individual Level

7. **Mobile computing.**

- Always maintain physical control of mobile devices
- Disable wireless functionality when not in use
- Use separate personal and business mobile devices and accounts.
- Do not leave devices unattended.

Mobile Phone Security

- Android
  - You can download apps from anywhere and you can root your device.
  - If you're downloading from unknown sites or rooting your devices, you should consider an antivirus app.



Incoming phone calls
Hide private contacts' names and photos on security lock screen ☑

Passwords

Make passwords visible ☑

Device administration

Device administrators
View or deactivate device administrators

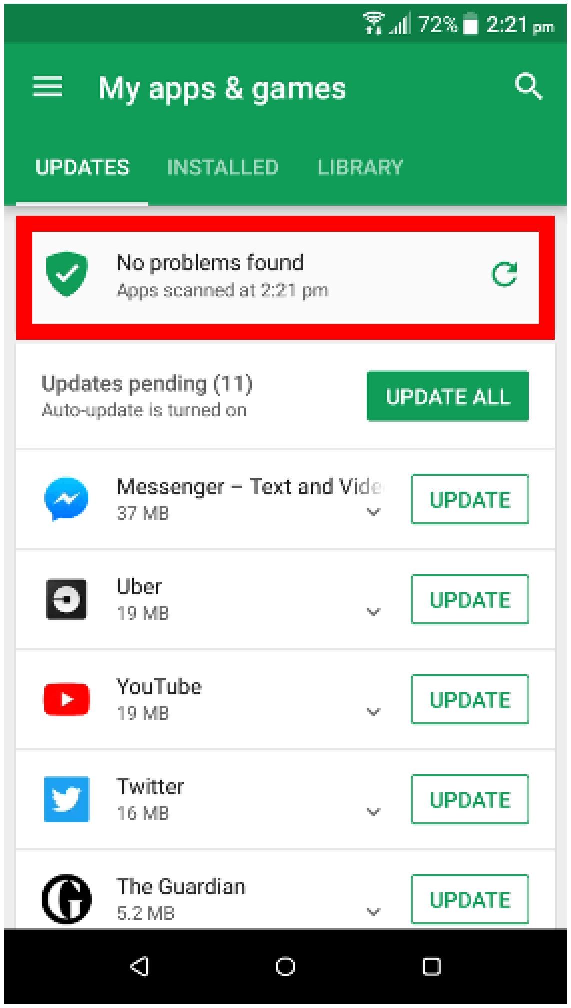
Unknown sources
Allow installation of apps from unknown sources ☑

Credential storage

Storage type
Hardware-backed

Mobile Phone Security

- Android
  - Use Play Protect to scan your device for malicious apps.



No problems found
Apps scanned at 2:21 pm

Updates pending (11)
Auto-update is turned on

Messenger – Text and Vide
37 MB

Uber
19 MB

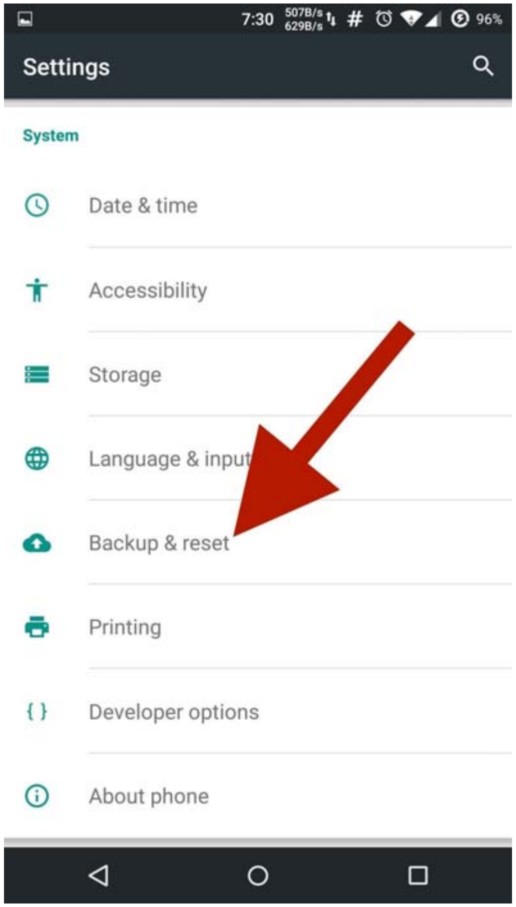
YouTube
19 MB

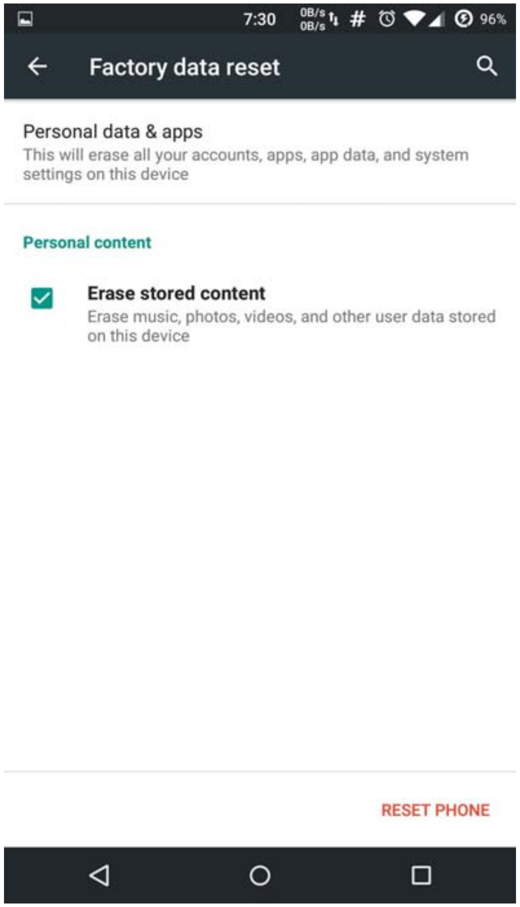
Twitter
16 MB

The Guardian
5.2 MB

Mobile Phone Security

- Android
  - If your device gets a virus, a factory reset should solve the problem.





Personal data & apps

This will erase all your accounts, apps, app data, and system settings on this device

Personal content

☑ Erase stored content

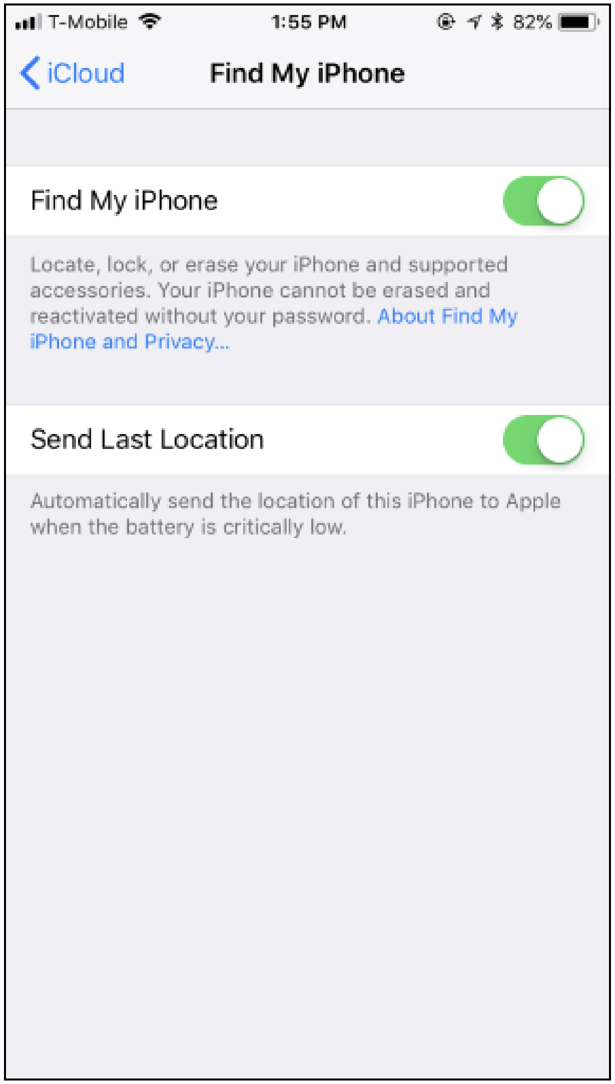
Erase music, photos, videos, and other user data stored on this device

Mobile Phone Security

- iPhone
  - Apps on your iPhone run in a sandbox.
  - “Security” apps are forced to run in the same sandbox.
  - “Security” apps can’t see a list of apps you’ve installed and can’t scan anything on your device for malware.

Mobile Phone Security

- How your iPhone protects you



T-Mobile 1:55 PM 82%

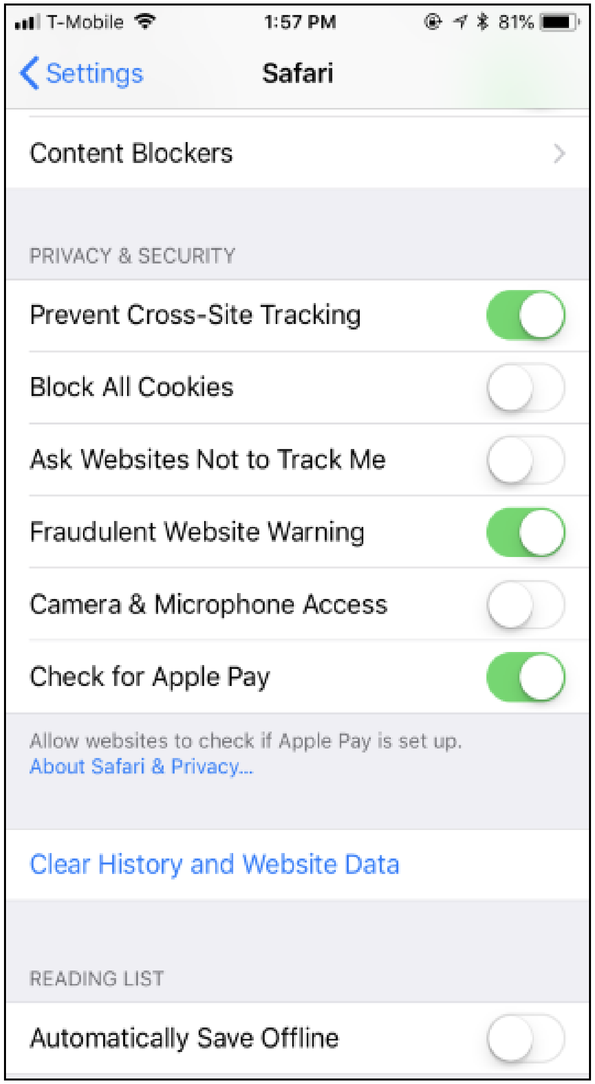
iCloud — Find My iPhone

Find My iPhone ●

Locate, lock, or erase your iPhone and supported accessories. Your iPhone cannot be erased and reactivated without your password. About Find My iPhone and Privacy...

Send Last Location ●

Automatically send the location of this iPhone to Apple when the battery is critically low.



T-Mobile 1:57 PM 81%

Settings — Safari

Content Blockers ›

PRIVACY & SECURITY

Prevent Cross-Site Tracking ●

Block All Cookies ○

Ask Websites Not to Track Me ○

Fraudulent Website Warning ●

Camera & Microphone Access ○

Check for Apple Pay ●

Allow websites to check if Apple Pay is set up. About Safari & Privacy...

Clear History and Website Data

READING LIST

Automatically Save Offline ○

Mobile Phone Security

- iPhone
  - iPhone devices can only install apps from Apple’s App Store.
  - “Find My iPhone” functionality lets you remotely locate, lock, or erase a lost or stolen iPhone.
  - “Fraudulent website warning” presents you with a warning if you end up on a malicious website.
  - DON’T JAILBREAK YOUR IPHONE!!

Cindy Gross, CPA, CISA, C|EH

cgross@becpas.com

540 434-6736

Save the Children Federation

An international not-for-profit organization working to save underprivileged children.

- What happened?
  - A worker's email was hacked, allowing the hacker to pose as an employee and create fake invoices.
- Impact
  - The organization paid approximately $1 million to fake invoices. The organization recovered all but $112,000 due to insurance coverage.

Save the Children Federation

- Impact
  - Implemented controls that involved a second staff member to confirm all new vendors.
  - Expenditures to strengthen technology systems.
  - Instituted a requirement that a second person sign off on wire transfers.

thank
you