Everyday Cybersecurity

17 Doable To-Dos

Craig Jackson, Chief Policy Analyst, CACR
Susan Sons, Senior Security Analyst, CACR
cacr.iu.edu

29 Sep 2016 - CACR Summit

CENTER FOR APPLIED
CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

Today's goal

Give you any connected adult a handful of doable cybersecurity measures that many people haven't yet taken -- measures that will make your lives significantly more secure.

How did we come up with this stuff?

We selected to-do's in order to maximize:

positive impact x *doability*

This list represents CACR's extensive knowledge of best practices, security policy and regulations, security research, and experience in helping people.

Important caveats:

A. CACR's list is likely to change as time passes. New types of attacks will emerge. New or easier-to-use defenses will help.
B. There are a lot of good practices that didn't make the cut, because they are too challenging to accomplish and/or don't have as big a return on investment.

17 To-Do’s

1. Lock Your Screens

On your phone

On your computer

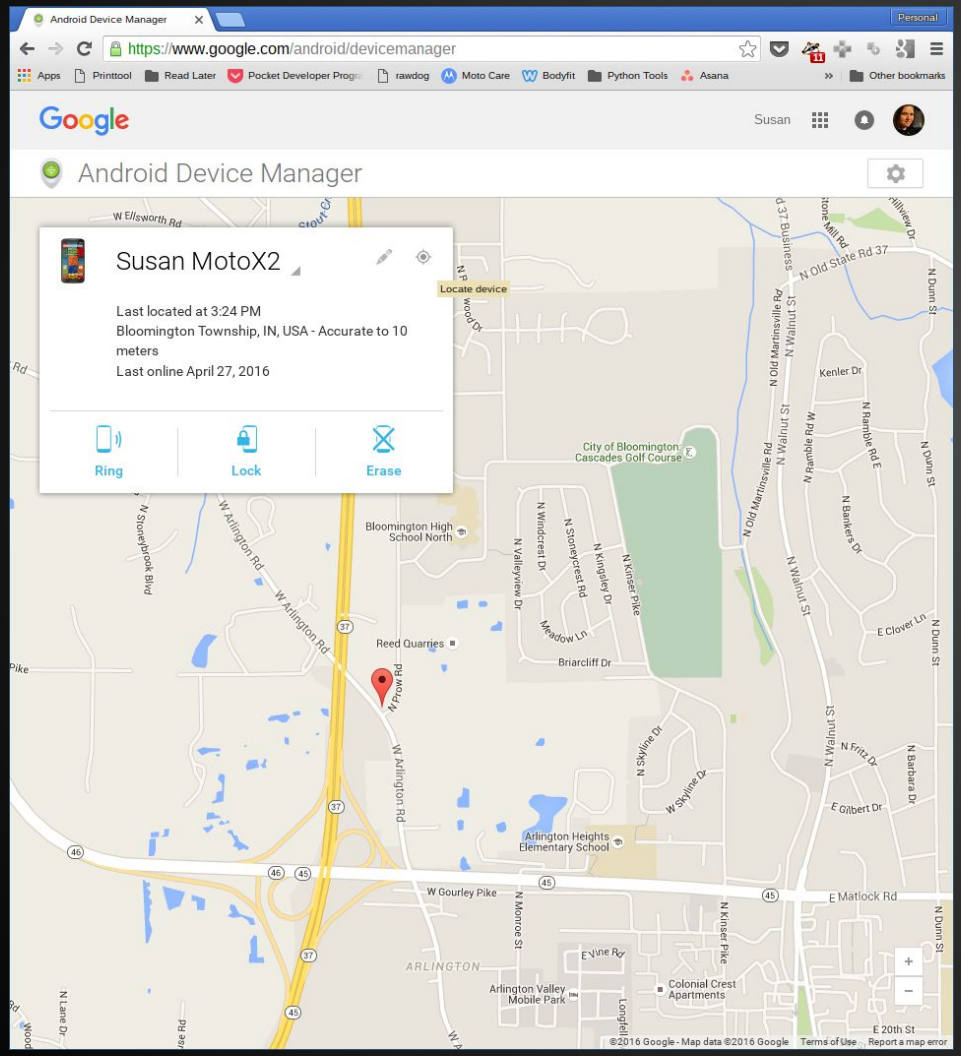
EVERY time you pocket the device or step away.

Otherwise, anyone who picks up your device gets all your data, and the ability to impersonate you.

2. Use Full Disk Encryption Everywhere

Without full disk encryption, an attacker can take your phone or computer and, ignoring the system password, remove the storage device and copy all of the data off to another system.

3. Use a Remote Device Manager



Find your lost device, lock it, or wipe it before a thief gets your data.

4. Keep Regular, Secure Back-Ups

Backups protect you from accidental deletions. Moreover, in the case of a destructive virus or ransomware, solid backups give you the ability to throw up your hands, erase everything, and re-install from scratch (done!) instead of requiring expensive, time-consuming, and technically complex recovery and restoration tactics.

Backups should be protected at least as well as the places the data came from.

5. Take Software Updates Seriously

Apply software updates regularly, and JUST SAY NO to end-of-life (EOL) software.

When a security bug gets patched, it is publicly known, and (if not already being exploited in the wild), it will be seen in mass, untargeted attacks within 6-24 hours. Failing to apply patches promptly means guaranteeing the bad guys have a way into your system.

EOL software doesn't get patches, even when known security vulnerabilities exist…need we say more?

6. Isolate User Accounts

Ideally, one should only have one person using each device, and that user NEVER logs in as administrator unless doing an administrative task.

In the real world, one computer, one tablet, etc. per person may not be realistic at home: in this case, each user MUST have their own login account on the machine, and the administrator account should not be anyone's "daily driver".

Separating users protects users' data from one another's activities and mistakes, and separating the admin makes the machine harder to compromise. E.g., a child playing an insecure flash game is less likely to release your tax returns to the internet.

7. Monitor Your Financial & Sensitive Accounts

Two things:

1. Set notifications.
2. Review your bills, line by line, unless your notifications work really well.

Why?

a. Financial institutions are watching things more closely, but they don't catch everything.
b. You can only take action on fraudulent charges if you know they occurred.
c. Even more important for small businesses!

8. Use Your Credit Card

Why?

a. Credit card companies, and in some cases merchants, hold the bag on fraudulent charges against your account. It's the law!
b. Fewer protections on your debit card / bank account.

Need to carry your debit card for ATM purposes? Check for ATM machine tampering; cover the keypad while typing.

9. Freeze Your Credit

Get your free credit report, review everything, deal with any issues, then FREEZE IT at all three bureaus. (Do this for your kids too!)

Why?

a. Identity theft happens, and if it happens to you and impacts your credit, you are in a mess.
b. It's free.
c. Monitoring companies have a mixed track record.
d. Lifting freezes is pretty easy.
e. Recommended by our Indiana Attorney General.

10. Store Your Passwords in a Safe Place

This probably means using a password manager like 1Password, LastPass, KeePass.

This probably means using a strong passphrase for your highest sensitivity accounts, *e.g.*, the master pw for your password manager.

Why?

a. Most people need to get to their pw's from a variety of places. (What about on paper?)
b. Good pw's are *unique* and *strong*… so you'll have a bunch that you can't remember.

11. Use Unique Passwords

Never reuse the same password or PIN.

Why? Imagine the Netflix password database falls off a truck…. Did someone just get the password for your bank account?

Passwords should be substantially different. Don't just change one character or number.

Why? Attackers know that people often just use variations.

12. Use Strong, Hard-to-Guess Passwords

Password: `9!rDzQ@wQUKuG!E^Fr#aPm9U6K$XzP`

Passphrase: `animal7 encourage telex48 nuisance`

Why?

a. They need to be resistant to both human guessing and machine “cracking.”

Why ever use a *passphrase*? You can remember it and avoid writing down anywhere, but it is long, and (hopefully) hard to guess/crack. Do *not* use your kids’ names, your birthday, or “GoColts.”

13. Use 2-Factor Authentication

For your most sensitive online accounts, find out if multifactor (aka 2 factor) is available and get it activated. Often described as “something you know / something you have.” (If it is not available, request it!! Demand it! Send a certified letter quoting Kamala Harris.)

Why?

a. Even if you do a great job of creating and storing passwords, attackers find ways snatch them.
b. Some organizations do a bad job of protecting your passwords.
c. Huge peace-of-mind lift.

14. Become Scam-Resistant

The vast majority of successful attacks start with someone voluntarily giving up information they should not have, for example:

- Putting a username/password in a scammer's web form.
- Giving out personal information on the telephone.
- Putting paperwork or disk drives with sensitive information in the trash.
- Selling a phone or computer without scrubbing personal information off completely.
- Entering sensitive information on a "legitimate" web site that is not well secured.
- Free phishing tutorial at: https://goo.gl/iIxhRA

15. Treat Email Like a Postcard

- Assuming that the parties to an email aren't all using end-to-end encryption, at least the sender's and receivers' email servers can read your email…as can the people who own and maintain them.

- In the typical case, many internet waypoints in between can read it as well, and you don't control which waypoints see your mail.

- Even when email is encrypted, it's like a sealed letter: anyone can read the information on the outside of the envelope: such as the to/from information, postmark date, and so on.

- Would you risk sending passwords, credit card numbers, SSNs and other sensitive information on a postcard to an unsecured (not locked) mailbox on the street?

16. Beware the Creep of Internet of Things

- More devices are becoming network-connected every day, usually with very little thought paid to security.
- IoT devices may be impossible to patch once security vulnerabilities are found.
- EVERY network-connected device is a potential entry point to the network, and many have sensors that reveal data about the physical home or office.
  - The thermostat that tells strangers on the internet when you are home.
  - The nanny cam that allows anyone to view activity in your home.
  - The scale that gives access to all of your network traffic to an intruder.

17. Help Family Members Secure Themselves

- “Network nannies” are easy to circumvent, and won’t be in place on every computing device your child sees.
- Kids learn to protect themselves by doing so under the guidance of a patient adult.
- Young children are generally more receptive than teens: teaching good habits early is less work.
- Seniors are often at greater risk than kids, as they have a bigger learning curve when dealing with tech.
- Have concrete goals: “be safe” is too vague to ask of anyone.

The To-Do List

1. Lock Your Screens
2. Use Full-Disk Encryption Everywhere
3. Use a Remote Device Manager
4. Keep Regular, Secure Backups
5. Take Software Updates Seriously
6. Isolate User Accounts
7. Monitor Your Financial & Sensitive Accounts
8. Use Your Credit Card
9. Freeze Your Credit
10. Store Your Passwords in a Safe Place
11. Use Unique Passwords
12. Use Strong, Hard-to-Guess Passwords
13. Use 2-Factor Authentication
14. Become Scam Resistant
15. Treat Email Like a Postcard
16. Beware the Creep of the Internet of Things
17. Help Family Members Secure Themselves

Resources

Stop. Think. Connect.
https://www.dhs.gov/stopthinkconnect

SANS “Ouch” Series
http://securingthehuman.sans.org/resources/newsletters/ouch/2016

CACR’s Security Matters Series
https://www.youtube.com/user/cacrsecuritymatters

Thank you.

Craig Jackson, scjackso@indiana.edu
Susan Sons, sesons@iu.edu

Slides at: http://cacr.iu.edu/2016summit

Many thanks to our colleagues at CACR (Ryan Kiser, Mark Krenz, Scott Russell, Anurag Shankar, Amy Starzynski-Coddens, Von Welch) and IU (Ian Washburn, Matt Estell) for their contributions and comments.

cacr.iu.edu/give