EFF SEC Lessons

Today's Lesson:

Locking Down Social Media

Presented by: Cryptoparty Ann Arbor

https://a2crypto.party

https://sec.eff.org / https://ssd.eff.org

Last Updated: 3/7/2020

Cryptoparty Ann Arbor

CryptoParty Ann Arbor (Michigan) is a community of privacy-minded educators, techies, activists, and enthusiasts working to help you reclaim your privacy.
We put people first, and see within technology the potential for liberatory social change.

We ARE THE CryptoParty Ann Arbor!

– https://a2crypto.party

Event Expectations

Cryptoparty Ann Arbor events are intended to be inclusive and welcoming for everyone. In particular, we do not tolerate harassment of participants, whether attendees, guests or our staff, in any form.
Please see: https://we.riseup.net/a2cryptoparty/event-expectations

We may call on some people to provide verbal responses at times.
Any participation is entirely voluntary.
Please feel welcome to submit written questions.
Please let us know if you need any accommodations.

AADL Event Expectations

Ann Arbor District Library Rules of Behavior:
https://aadl.org/aboutus/policies/behavior

Facilities Use by the Public - MEETING ROOM POLICY:
https://aadl.org/aboutus/facilities#MEETING

We are holding this event in the Library, but we are NOT THE Library!

Cryptoparty?

CryptoParty is a decentralized movement with events happening all over the world. The goal is to pass on knowledge about protecting yourself in the digital space. This can include encrypted communication, preventing being tracked while browsing the web, and general security advice regarding computers and smartphones.

We are an Ann Arbor collective of CryptoParty, NOT THE CryptoParty!

– https://cryptoparty.in

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

WE ARE NOT THE EFF!

-https://eff.org

Electronic Frontier Alliance

Cryptoparty Ann Arbor is a proud member of the Electronic Frontier Alliance (EFA)!

We are a MEMBER of the EFA, not THE EFA

As a member organization of the EFA, we believe that technology should support the intellectual freedom at the heart of a democratic society. In the digital age, that entails advancing: Free Expression, Security, Privacy, Creativity, and Access to Knowledge

– https://eff.org/efa

Security Education Companion

The Security Education Companion (SEC) is a resource by The EFF for people teaching digital security to their friends and neighbors.

Lesson modules are centered around specific learning objectives:

- Threat Modeling (Security Planning / Risk Assessment)
- Phishing and Malware
- Two-Factor Authentication
- Passwords
- More: https://sec.eff.org/topics
- Surveillance Self-Defense: https://ssd.eff.org

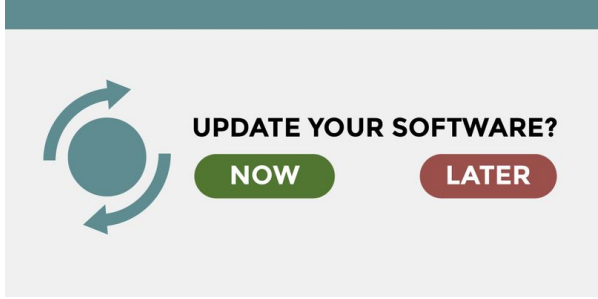
Basics - BACKUPS

The **3-2-1 rule of backups**:
3 – Keep 3 copies of any important file: 1 primary and 2 backups.
2 – Keep the files on 2 different media types to protect against different types of hazards.
1 – Store 1 copy offsite (e.g., outside your home or business facility).
https://www.backblaze.com/blog/the-3-2-1-backup-strategy/

You may need to Save As / Export / Download your data, especially if using Cloud services such as Google, Office 365, etc.

Cryptoparty Ann Arbor Links - Backups
https://we.riseup.net/a2cryptoparty/links#backups

Basics - UPDATES



Software Updates and Why They're Important

“Keep your software updated!” is the closest thing we have to security advice that will work for everyone. By keeping your software up to date at all times, you’re staying one step ahead of all but the most advanced threats.

https://sec.eff.org/articles/software-updates

Updates: smaller, more frequent, bug and security fixes (1.0 to 1.1)
Upgrades: larger, less frequent, new features (1.0 to v2.0)

Cryptoparty Ann Arbor Links - Updates

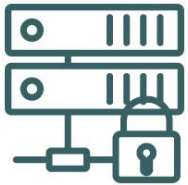
https://we.riseup.net/a2cryptoparty/links#updates

Basics - 2FA & PASSWORDS

2FA - 2 Factor Authentication:

- Enable 2FA in as many places as you can: https://authy.com/guides
- Google Authenticator: Use **Authy** or **DUO Mobile** instead for **backup**

Passwords:



- Use **different** passwords **every account**
- **Generate** (don't THINK of) passwords if at all possible using:
  a. **A Password Manager**: LastPass, 1Password, Dashlane, KeePassXC, Blur, etc.
  b. **Diceware** is great for sharing, memory, and typing: https://www.eff.org/dice

- A paper notebook ***with strong physical security*** can work great until you can start using a Password Manager.

Today's Lesson:
Locking Down Social Media

https://sec.eff.org/topics/locking-down-social-media

Using social media safely and comfortably is an ongoing challenge for many learners. In this lesson, we'll go over some basic concepts and things to watch out for on social media websites and settings.

Accompanying guide:
https://ssd.eff.org/en/module/protecting-yourself-social-networks

Locking Down Social Media - Ice Breaker

Raise your hand if you've used a social media platform once today.

- How about twice?
- How about three times?

Locking Down Social Media - Warmup

Split into pairs or small groups and talk about your favorite use of social media.

Examples include: sharing pictures, organizing events, staying in touch with long-distance family and friends, participating in online communities, spreading their art/work/activism, etc.

Locking Down Social Media: Knowledge Share

What is personally Identifying Information (PII)?

- PII, sometimes called “Sensitive Personal Information” or “Potentially Identifying Information,” is information that can be used to identify a person. It might be combined with other information to figure out someone’s location, to contact them, or to gather additional information about their life. Lots of companies collect this information for many purposes, including advertising, medical documentation, or billing.

Locking Down Social Media: Knowledge Share

Don’t blame yourself!

- We don’t want you to blame yourself for what big tech companies and social media platforms have done to your privacy!
- Instead, we can help you focus on small but powerful actions you can take to reclaim their privacy.

Locking Down Social Media: Knowledge Share

Security and privacy “check-ups”

- Facebook, Google, and other major websites offer “security check-up” features. These tutorial-style guides walk you through common privacy and security settings in plain language and are an excellent feature to take advantage of… when available … if you can find it!

Locking Down Social Media: Knowledge Share

Privacy vs. security; safety vs. account settings

- Privacy settings tend to answer the question: “Who can see what?” Here you’ll probably find settings concerning audience defaults (“public,” “friends of friends,” “friends only,” etc.), location, in photos, contact information, tagging, and if/how people can find your profile in searches.
- Security (sometimes called “safety”) settings will probably have more to do with blocking/muting other accounts, and if/how you want to be notified if there is an unauthorized attempt to authorize your account.

Locking Down Social Media: Knowledge Share

Location

- Location settings help you make sure that you don’t accidentally share where you are. Some sites will include your approximate location by default when you post things.
- Location information can paint a detailed picture of your habits, home, and workplace, so it’s important to turn off if it’s leaking information that you feel uncomfortable with.

Locking Down Social Media: Knowledge Share

Photos

- Photos can share more information than meets the eye. In addition to metadata that might include the time and place a photo was taken, the image itself can provide some information. Before you post a picture, ask:
  - Was it taken outside your home or workplace?
  - Are there any addresses or street signs visible in it?
  - If you post photos often at certain times of day, does it make it easy to figure out what your routines and habits might be?
- Photos can also link accounts you intend to keep separate. Be sure to use a photo or image that you don’t use anywhere else online.

Locking Down Social Media: Knowledge Share

Making sure different profiles don’t get linked together

- Dating websites, professional profiles, anonymous accounts, accounts in various communities, etc.
- Potentially linking variables to watch out for include: phone number, pictures, your name (including nicknames), your email, etc.
- It can be easy to get scared or panic when you find your information where you don’t want it. Instead of trying to wipe all information about you off the entire Internet, just focus on specific pieces of information, where they are, and what you can do about them.
- Be aware of Group settings vs. Personal settings

Firefox Facebook Container

https://www.mozilla.org/en-US/firefox/facebookcontainer/

- Facebook can track almost all your web activity and tie it to your Facebook identity. If that's too much for you, the Facebook Container extension isolates your identity into a separate container tab, making it harder for Facebook to track you on the web outside of Facebook.
- Facebook will still be able to send you advertising and recommendations on their site, but it will be much harder for Facebook to use your activity collected off Facebook to send you ads and other targeted messages.

Jumbo

Free iOS / Android service that connects to your social media accounts and helps you manage posts and privacy settings.

- https://jumboprivacy.com
- Available Apps: Facebook, Facebook Messenger, Google, Gmail, YouTube, Google Maps, Google Chrome, Data Breach (E-Mail Address), Twitter, Amazon, Alexa

Umbrella Security

Free digital and physical security advice App

- https://secfirst.org/umbrella
- Feeds, Forms, Checklists, and Lessons:
  - Lesson for Online Privacy
    - Beginner: I want to ensure my privacy when using social media
    - Advanced: I need to stay anonymous online.
  - Other Lessons:
    - Assess Your Risk, Information, Communications, Travel, Work, Incident Response, Stress, Emergency Support, Tools
  - Forms: Digital Security Incident, Physical Security Incident, Proof of Life Form, Travel Security Memo

iVerify

Paid ($2.99) iOS App that monitors your device security, notifies you when an issue is detected, and provides actionable steps to take to mitigate any risks.

- https://iverify.trailofbits.com
- Checklists include:
  - Protect against theft
  - Limit software exploits
  - Prevent data leakage
  - Review for signs of compromise
  - Use good security software
  - Secure your online accounts
  - Network security (Advanced)

Extra Time

Now that we've completed the lesson (and have some additional time!), we can continue the discussion of today's topic and/or go into others.

Examples:

- Additional Privacy Apps & Services (Extra Slides)
- Security Plan (Threat Model / Risk Assessment)
- Two-factor Authentication
- Password Managers
- Secure Messaging

Thanks / Feedback / Getting Involved

Whether you're simply curious or want to start a technical revolution, we encourage you to get in touch with us physically or electronically. The only time conditions change is when we band together to change them.

- a2crypto.party: Our website.
- E-mail: cryptopartyannarbor@riseup.net
- Discussion List: https://autistici.org/mailman/listinfo/cryptoparty-ann-arbor
- Announcements https://lists.riseup.net/www/info/cryptoparty-a2-announce
- Twitter - @CryptopartyAA
- Facebook - a2cryptoparty

Browser Add-ons, Extensions

Privacy Badger

- https://www.eff.org/privacybadger

HTTPS Everywhere

- https://www.eff.org/https-everywhere

uBlock Origin

- https://github.com/gorhill/uBlock

Firefox (by Mozilla)

Firefox products are designed to protect your privacy:

- https://www.mozilla.org/en-US/firefox

Firefox Personal Data Promise: Take less. Keep it safe. No secrets:

- https://www.mozilla.org/en-US/firefox/privacy

One login. All your devices. A family of products that respect your privacy:

- https://accounts.firefox.com

Firefox Mobile / Focus

Firefox Mobile (iOS / Android)

- https://www.mozilla.org/en-US/firefox/mobile/
- Super fast. Private by default. Blocks 2000+ online trackers.

Firefox Focus (iOS / Android)

- https://support.mozilla.org/en-US/products/focus-firefox
- You can use Firefox Focus as a standalone browser or as content blocker for Safari on iOS

Multi-Account Containers

Firefox

https://support.mozilla.org/en-US/kb/containers

- Just like the Facebook Container but for Personal, Work, Banking, Shopping, etc.
- Container tabs are like normal tabs except that the sites you visit will have access to a separate slice of the browser's storage.
- This means your site preferences, logged in sessions, and advertising tracking data won't carry over to the new container.
- Likewise, any browsing you do within the new container will not affect your logged in sessions, or tracking data of your other containers.

Abine Blur

https://www.abine.com

- Free: Encrypted Passwords (Password Manager), Masked Emails, Tracker blocking, Auto-fill
- **Premium (PAID)**: Masked Cards (virtual cards), Masked Phone, Backup & Sync

Abine DeleteMe

https://joindeleteme.com

- ***PAID SERVICE*** DeleteMe removes your personal information like name, address, age, phone number, email address, and photos of your home from leading data broker sites. Removing personal information from data broker websites reduces your online footprint, and removes Google search results.

Free DIY Opt-Out Guide (can be very tedious & time consuming!):

- https://joindeleteme.com/help/diy-free-opt-out-guide/

Security Checklist

Security Checklist

https://securitycheckli.st

- An open source checklist of resources designed to improve your online privacy and security.
- Check things off to keep track as you go.
- A beginner’s checklist for staying safe on the internet.

PrivacyTools

https://www.privacytools.io

- We provide services, tools, and knowledge to protect your privacy against global mass surveillance, and moderate a thriving community of privacy-minded individuals like yourself to discuss and learn about new advances in protecting your online data. This website serves as the centerpiece of our organization, where we research and recommend various software solutions for our community.