Digital Tools to Keep Your Work Safe

Mike Tigas
(@mtigas)
News Applications Developer, ProPublica


https://bitly.com/dcAMP-securitytools
Data at rest. What's on your computer? What's sitting in your e-mail archive?
Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data in motion. Calls, messages, files sent; anything out of your hands.
How Email Appears to Work

Sender's Outbox -> Recipient's Inbox

How Email Really Works

Sender's Mail Client (MUA) -> Sender's MDA/MTA

Company Network

Sender's Mail Server (MTA)

email queue

Router

The Internet

Router

Recipient's MDA/MTA

Recipient's Mail Client (MUA)

Recipient's Mail Server(s) (MTA)

Spam & Virus Blockers

https://www.oasis-open.org/khelp/kmlm/user_help/html/how_email_works.html
https://en.wikipedia.org/wiki/Grumman_LLV
John H. Atlerton
Dept. of Anth.
Portland State U.
P.O.Box 751
Portland, Oregon, 97207
U.S.A.

https://commons.wikimedia.org/wiki/File:Airmail_envelope_from_Kabala,_Sierra_Leone_%28West_Africa%29_to_Portland,_Oregon_%28USA%29_%283710984093%29.jpg
Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data in motion. Calls, messages, files sent; anything out of your hands.

Metadata. Who are you talking to & when. How big are those files/msgs?

http://www.salon.com/2013/04/24/how_a_twitter_hack_sent_the_market_plummeting_ap/
Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data in motion. Calls, messages, files sent; anything out of your hands.

Metadata. Who are you talking to & when. How big are those files/msgs?

Identities & logins.
“Perfectly secure” doesn't exist.
Humans are insecure
A CRYPTO NERD'S IMAGINATION:

His laptop's encrypted. Let's build a million-dollar cluster to crack it.

No good! It's 4096-bit RSA!

Blast! Our evil plan is foiled!

WHAT WOULD ACTUALLY HAPPEN:

His laptop's encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
Hello,

Please read the following article, it's very important:


[A different AP staffer]
Associated Press
San Diego
mobile [removed]
Microsoft Outlook Web App

Your session has timed out. To protect your account from unauthorized access, the connection to your mailbox is closed after a period of inactivity. Please re-enter your user name and password.

Security (show explanation)

☐ This is a public or shared computer
☐ This is a private computer
☐ Use the light version of Outlook Web App

Domain\user name: ________________________________
Password: ________________________________

Sign in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.
First:

- Passwords
- Software updates
- Antivirus / antispyware
- Web browsers
Passwords

• Don't use the same couple of passwords everywhere.

• If your company e-mail is secure but you use the same (or a similar) password on shadywebsite.info, you’ve done the evil hacker's job for them.
Password Managers

• Helps you use a different, absurdly long password everywhere

• **1Password** (Mac/iOS/Windows)
• **LastPass** (multiplatform, website)
• **KeePassX** (multiplatform app)
Software updates

• Security holes in Windows, Mac, and Linux, are discovered on a near-daily basis. Same with browsers and most other software.

• Sometimes, a security hole just needs you visit a web page and you're toast.
Antivirus/antispyware

• Not as relevant anymore, since advanced "crypting" techniques can mask malware from detection.
• But still provides protection from shotgun-style attacks.
Web Browsers

- Firefox & Chrome update themselves automatically
  - Make sure it updates: Close your browser when you're done using it!

- Most modern browsers have a “warn if this is a shady website” feature.
Web Browsers

• “Click To Play” for plugins.
  • Only lets multimedia open in your browser when you've asked for it.
  • Chrome, Firefox, Safari

• HTTPS Everywhere (Firefox & Chrome)
  • Redirects you to the secure version of a website, if one exists.
Data At Rest

- Deleting files safely
- Encrypting files
- Encrypting your entire computer
Secure deletion

• When you delete a file from your computer, you’re only striking it from the “table of contents” of your drive.

• Data still there until something else needs to use those unused “pages.”

• A “secure” delete writes random data into the place where the file was.
Secure deletion

• “Secure Empty Trash” on Mac
  • Hold ⌘ key when right-clicking Trash.

• Disk Utility (Mac)
• CCleaner (Windows)
File encryption

- Protects files
- Use case: sending sensitive files or putting files on USB sticks to share.

- TrueCrypt (multiplatform)
- MiniLock (multiplatform)
Full disk encryption

- Protects all data on your computer, when computer is turned off.
- Use case: Protects if computer is stolen

- Apple FileVault (Mac)
- Microsoft BitLocker (Windows)
- TrueCrypt (Windows)
FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".

Click the lock to prevent further changes.
Data In Motion

• Web Browsing
• Texting & Instant Messaging
• Phone calls, Voice/Video chat
• E-mail
Web Browsing: Tor

• Anonymizes your internet connection so websites don’t know where you are

• Relays your web traffic through other computers before going to the website you are trying to access

• Caveats:
  • Slower
  • Last computer in the chain can see what you’re doing – unless encrypted. (They'll still have metadata.)
Tor

- PC/Mac/Linux: [https://www.torproject.org/ “Tor Browser Bundle”](https://www.torproject.org/)

- iOS: [Onion Browser](https://www.torproject.org/)
  (disclosure: I work on this)

- Android: [Orbot](https://www.torproject.org/)
Public Key Encryption

• Say you need to share something or send a message to someone?
• You can encrypt it, but you need a password.
• https://www.youtube.com/watch?v=YEBfamv-_do&t=2m15s
Chat: OTR Encryption

- Apps for instant messaging that encrypt messages between you and someone else.
- Can often use an existing account (like Google Chat) & use an OTR app through that.

Caveats:
- Metadata – information about who you are talking to and when – is still seen
OTR Encryption

Jeremy B. Merrill

Mike Tigas

Jeremy B. Merrill
OTR Encryption

- Mac: **Adium**
- Windows: **Pidgin + OTR plugin** ("Win32 installer")
- Setup Guides:  
  - Hacks/Hackers NYC (Mac)  
  - Security in a Box (Windows)  
  - Freedom of the Press Foundation
Chat: Encrypting Texts

• Apps that act like text messaging. Non-OTR, but very similar:
  • **TextSecure** (Android) & **Signal** (iOS; texting coming soon)
  • IOS: iMessage encrypts, but Apple may have access. Messages may be logged.

• Normal OTR app:
  • IOS & Android: **ChatSecure**
Voice/Video Calls

• FaceTime: See iMessage. Prevents cell provider from knowing who you call, but Apple may have access.

• Phone:
  • Signal (iOS) & RedPhone (Android)
  • Both: SilentCircle ($$$)

• Skype-like:
  • Ostel service, with choice of apps for Win/Mac/iOS/Android
E-mail: PGP

- “Pretty Good Privacy”
- Also known as GPG — for “GnuPG”, one of the programs that does this
- Public and private keys, you have to download someone's public key to send them an encrypted message.
PGP

• Can encrypt files & messages. • Only the recipients you choose can ever decrypt it.

• “Signing” feature adds a digital fingerprint to a message that says that 1) you actually sent this message 2) message wasn't tampered with.
PGP

• Mac:
  GPGTools + Thunderbird + Enigmail

• Windows:
  GPG4Win + Thunderbird + Enigmail

• Setup guides:
  Hacks/Hackers NYC
  Freedom of the Press Foundation
  Security in a Box
Advanced Tools

- **Tails** — A totally isolated operating system that you run on your computer via a thumbdrive or CD. Tunnels through Tor by default, comes with many secure communication tools installed.
Try these today

• Use a password manager
• Download Tor Browser Bundle
• Set up RedPhone (Android) / Signal (iOS) and find a buddy who also has it. Make an encrypted phone call.
If you have an hour

• Turn on FileVault (Mac). Plug your computer in when you do this, it might take an hour or two.

• Set up an instant messaging app and set up OTR with your GChat (if you have one).

• Try MiniLock. Have a friend install it too, then encrypt a file for them and e-mail it.
If you have a while

• Set up PGP; generate a key, share it with someone (like me!), see if you can send each other encrypted messages.