Digital Security for the 2017 Lawyer

Presentation for the BC Courthouse Libraries on April 25th, 2017

Disconnected?

Go to **jointraining.com**
Training ID: **812-454-908**

Digital Security for the 2017 Lawyer

Presentation for the BC Courthouse Libraries on April 25th, 2017

Your Host

Katrina Leung
Liaison Lawyer – Courthouse Libraries BC
kleung@courthouselibrary.ca

Who Am I?

- Toronto lawyer
  - https://www.cameronhuff.com
  - Typical clients: software developers & Bitcoin companies
- Past career: programming SaaS software
- Co-founder of several legaltech businesses
  - e.g. www.global-regulation.com

Addison Cameron-Huff

Six Topics: Six Slides

1. Phone
2. Computer
3. Website
4. Email
5. Meetings
6. Internet

Further reading & references at the end of the presentation.

Your Phone

- Enable disk encryption (for Android)
  - New iPhones come with this by default
  - Data is encrypted “at rest”
- Set a PIN
  - Don’t make it 1234…
- Use a short timeout for screen locking
- SMS-based 2FA is a vulnerability
  - Use authenticator applications where possible
  - Phone companies are constantly being hacked through social engineering

Your Computer

- Encrypt your hard drive
- Computers with client files need strong passwords
- Have a short timeout
- Encrypt client files in a secure disk image
  - Only decrypt when you’re working on them
- Accounting is a target: use a dedicated computer if possible
  - Especially a concern if you’re accepting Bitcoin (future of payments?)
  - Consider buying a cheap Chromebook for this

Your Website

- Use SSL
  - This is transport encryption (not encryption at rest)
  - It’s free now with services like Let’s Encrypt (built into some shared hosting providers)
- Small/Solo Lawyer? Avoid Wordpress/Drupal
  - I used to make money building Wordpress sites for people & fixing hacks
  - It’s great but frequent vulnerabilities.
  - Can you secure it? Probably not.
- Consider a “static” site
  - You don’t want to be the lawyer serving malware to clients

Your Email

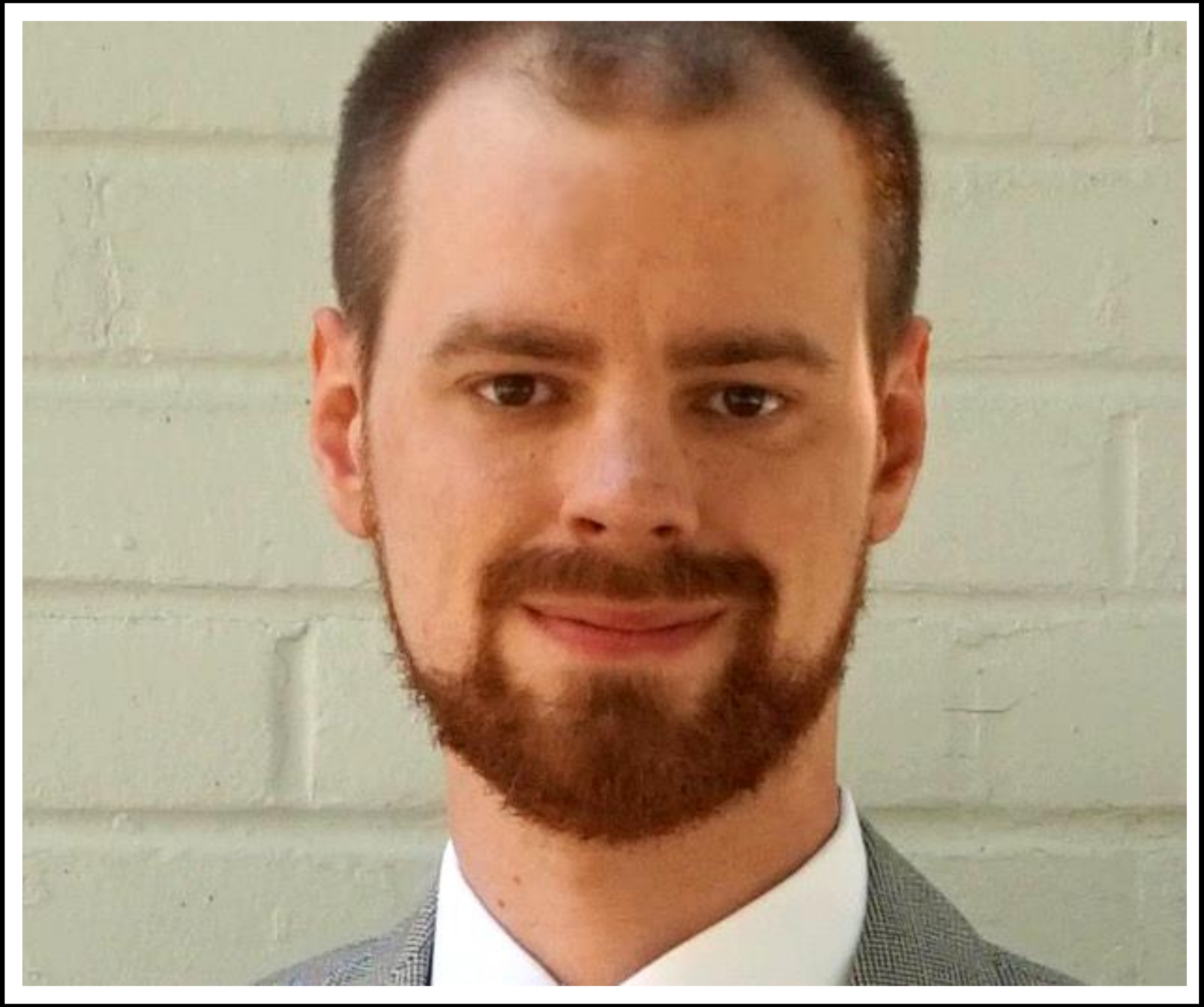
- Email is the main way lawyers communicate
  - Usually has some encryption along the way
- Consider SPF + DKIM
  - Improve deliverability of your emails
  - Improve the odds of a client detecting forged email
- If something needs to be delivered securely, consider other methods
  - Encrypted email systems exist but hard to use
  - Consider sending attachments inside encrypted disk images/password-protected ZIPs

Your Meetings

- In-person meetings are the most secure
  - I have incredibly tech savvy clients who insist upon it for important meetings
- I have a client who is a former military contractor
  - He insists that no phones or computers be taken into meetings
  - Are your meetings important? Consider doing what the experts do.
- Carefully consider Internet-connected devices in meeting rooms
  - IoT devices are often a weak-point in security – rarely patched
  - IP phones? Teleconferencing bridges

Your Internet

- Public wifi networks can be vulnerable to interception
- Consider using a VPN to connect to the Internet when out of office
  - VPNs can either be purchased or have an IT person set one up for you
  - Risk: the VPN provider could be spying on you
- Internet over cell service can also be intercepted
  - VPNs reduce this risk too
- HTTPS websites also help avoid interception
  - But a lock or green icon isn’t a guarantee
  - Need to know who the certificate was issued to



Questions?

Addison Cameron-Huff:
addison@cameronhuff.com

@acameronhuff on Twitter
www.cameronhuff.com/blog

Further Reading

- Krebs on Security: https://krebsonsecurity.com/
  - Blog about computer security with details about vulnerabilities
- David Whelan (Law Society of Upper Canada): https://ofaolain.com/
  - This is his personal blog, not LSUC, but it has good in-depth posts on security issues, from a lawyer's point of view
- The Intercept: https://theintercept.com/
  - News source that has in-depth coverage of state surveillance (same techniques can be applied by private attackers)
- Naked Security: https://nakedsecurity.sophos.com/
  - Computer security news source run by anti-virus company Sophos

References: Page 1/2

1. Android vs. iOS phone encryption: https://blog.cryptographyengineering.com/2016/11/24/android-n-encryption/

2. Phone 2FA: https://en.wikipedia.org/wiki/Multi-factor_authentication#Mobile_phone_two-factor_authentication

3. Demonstration of social engineering attack on phone company: https://www.youtube.com/watch?v=lc7scxvKQOo

4. Phone company social engineering leading to losses: https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#14eeb73f38ba

5. Enabling Windows encryption (BitLocker): https://support.microsoft.com/en-us/instantanswers/e7d75dd2-29c2-16ac-f03d-20cfdf54202f/turn-on-device-encryption

6. Creating an encrypted disk image on macOS: https://www.howtogeek.com/183826/how-to-create-an-encrypted-file-container-disk-image-on-a-mac/

7. How "air gapping" protects secure computers: https://en.wikipedia.org/wiki/Air_gap_(networking)

8. Toronto law firm's bookkeeper computer hacked, six figure loss: http://www.lawtimesnews.com/201301072127/headline-news/law-firms-trust-account-hacked-large-six-figure-taken

9. Chromebooks for sale: https://www.newegg.ca/Chromebooks/SubCategory/ID-3220

References: Page 2/2

10. Explanation of what SSL is and how it works: https://en.wikipedia.org/wiki/Transport_Layer_Security
11. Free SSL certificates from Let's Encrypt: https://letsencrypt.org/
12. Discussion of static vs. dynamic websites: https://www.quora.com/What-is-the-difference-between-Static-Websites-and-Dynamic-Websites
13. Enabling SPF & DKIM: https://mandrill.zendesk.com/hc/en-us/articles/205582267-About-SPF-and-DKIM
14. How PGP works for encryption (popular message encryption scheme): https://en.wikipedia.org/wiki/Pretty_Good_Privacy
15. Internet of Things as security weak point: https://www.ft.com/content/a63b2de8-992c-11e6-8f9b-70e3cabccfae
16. Tips for using public wifi networks: https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi
17. Why you can't rely on the "green bar" for SSL safety: https://www.wordfence.com/blog/2017/03/chrome-secure/
18. Airport wifi spying: http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

COURTHOUSE LIBRARIES | BC

Contact

training@courthouselibrary.ca

COURTHOUSE
LIBRARIES | BC

Thanks to our funders:

THE LAW
FOUNDATION
OF BRITISH COLUMBIA

THE LAW SOCIETY OF BRITISH COLUMBIA
INCORPORATED
18 84
LEX LIBERORUM REX

BRITISH
COLUMBIA

Ministry of
Justice