Digital Security and Journalism

FCC breakfast briefing
August 13, 2019

Dr. Lokman Tsui
School of Journalism and Communication
The Chinese University of Hong Kong
hi!

- professor at school of journalism, cuhk
- care about freedom of speech
- research on digital security and journalism
- previous research on internet censorship, personal data protection, journalism theory
- formerly at google
what do you do?
three typical attacks and what to do

- physical access to your phone
- spear phishing
- digital surveillance
physical access to your phone

- turn off Face ID and Touch ID
- turn on PIN, "erase data after ten attempts"
spear phishing

goals

• take over your device or account remotely
• reconnaissance

tips

• always keep your apps and OS up-to-date
• use 2-factor authentication (use app, not sms)
digital surveillance

- use end-to-end encryption
- "we kill people based on metadata"
- signal > whatsapp > telegram
- pay for a good VPN
caveats

• no "one-size-fits-all" security tips
• they become dated fast & often not timely
• prevention is good, but also have a plan for when you get hacked

digital security is like public health
provocation: digital security workshops are NOT very helpful in improving digital security

- not just about knowledge
- not even about skills

ultimately about changing behavior (like ... safe sex)
SAN FRANCISCO — The question is no longer who has been hacked. It’s who hasn’t?

The Washington Post can be added to the growing list of American news organizations whose computers have been penetrated by Chinese hackers.

After The New York Times reported on Wednesday that its computers as well as those of Bloomberg News had been attacked by Chinese hackers, The Wall Street Journal said on Thursday that it too had been a victim of Chinese cyberattacks.
so ... today any improvement?
state of digital security in hk local news orgs

tldr;

• state of digital security in hk news media "has room for improvement"

• poor support for digital security from news organization

• wide range of skills and mindsets, but "security by obscurity" is the norm

(tsui and lee, 2019)
mindset: security by obscurity

"I have no such experience before. I don’t think I have any secrets. Therefore I’m not a target for hacking. I haven’t worried about it before."

(tsui and lee, 2019)
mindset: security by obscurity

"There is no big issue in Hong Kong, I don’t think there is any."

(tsui and lee, 2019)
"Sometimes your boss joked that “even if the Chinese government does not read [your messages], the American government does. You think they don’t read your Gmail?” I would say “yes, but I’d rather they were read by the American government. Or my Kakao were being watched by the Korean government. I just don’t want them to be read by the Chinese government.”"
"We try our best to avoid phone calls and emails. It’s much better, thanks to 3G, 4G ... We used to use Gmail but since it was heavily cracked down, we’ve switched to instant messaging systems. We don’t have to use emails now. We actually explored many options to avoid using emails."

(tsui and lee, 2019)
mindset matters

"Yes, their awareness is poor. Resources will be provided after an attack, and it’s not costly, therefore I don’t blame on resources. If you ask me, I blame on the poor awareness. Very, very poor sense, a sense as if in the Stone Age."

(tsui and lee, 2019)
poor support from news organization

"In my opinion, on one thing, it [the IT department] would not set up a VPN for China reporting team. Some news organizations have it but we don’t. Yes, they then set up one, but it didn’t work that well. I ended up buying another VPN just in case."

(tsui and lee, 2019)
poor support from news organization
when asked about the use of VPN
"We use our own way. We don’t trust the company’s IT department! Same thing in every company! (Laugh)"
when asked if the company would pay for VPN
"The company won’t pay you for these things."
(tsui and lee, 2019)
but wait! i also have good news
THE PANAMA PAPERS

Politicians, Criminals and the Rogue Industry That Hides Their Cash
panama papers

• over 400 journalists and 120 news orgs working together
• successful in protecting source of data
• successful in protecting access to documents from attackers
• successful in preventing early disclosure
• successful in keeping project confidential and secret

(mcgregor et al. 2017)
panama papers: before

• almost half had never used two-factor
• almost half had never used PGP

(mcgregor et al. 2017)
panama papers: after

- everybody used two-factor
- everybody used PGP
- more than half said security compliance was "easy"

(mcgregor et al. 2017)
if you care about press freedom, you need to care about digital security

digital security means you get to cover stories you otherwise would miss out on
four things you and your org can do to improve digital sec

- reduce cognitive load
- know where to get timely support
- cultivate a culture of security
- be the internal advocate for better security policies
reduce cognitive load

- make security routine
- do not wait until you get hacked
- mandate 2-factor
- mandate end-to-end encryption
know where to get timely support

• appoint a digital security expert (your org has a media lawyer right?)

• journalists often have their own "person" for advice

• control quality of advice, lower cost for everyone
cultivate culture of security
break the taboo

• collect and share horror & success stories

"i do it because everyone else does it"

• provide transparency
• award good behavior
be the internal advocate for better security policies

"when I was there, at least the email system was encrypted, wi-fi system was improved, you know, the wifi format was WEP old format at that time, that crap. I told them to change, they didn’t approve to change to WPA enterprise level, so I hacked the system, forcing them to change it, simple."
digital security is a press freedom issue

press freedom under threat: yes

but also, digital security seen as press freedom: something we can (and should) daily exercise

good starting points for further security tips

• security planner https://securityplanner.org/#/ (by the citizen lab)

• TLDR guide to digital security https://github.com/hongkonggong/tldr-digital-security (by jason li)
thank you!

- lokman tsui
- email: lokman.tsui@gmail.com
- twitter: @lokmantsui

thanks to francis lee, masashi crete-nishihata, elizabeth watkins, jason li, the citizen lab and macarthur foundation