Securing Journalists

Runa Sandvik, Senior Director of Information Security
Introduction

- NYC since 2016 via DC, London, Trondheim, Oslo
- Hacked a wifi-powered sniper rifle in 2015 ✌
- Certified saké advisor as of October 2018 🍴
- Worked on Tor and SecureDrop, now at NYT
What’s this talk about?

- Threat models in the context of journalism and news media
- Challenges enhancing security for those we protect
- How to evaluate adversaries and their capabilities
- How we’re building a culture of security
Securing the newsroom

- The newsroom is very deadline-driven and product-focused
- Our journalists file from more than 150 countries each year
- Needs to click on links and open attachments
- The solutions we create have to be usable and reliable
- Need to raise awareness, build relationships, build trust
Combine that with...

- Individuals, desks, bureaus will have different threats and concerns
  - Investigations versus Obituaries
  - Moscow versus Los Angeles
- Individuals will have different levels of tech comfort / knowledge
- Individuals will have different workflows and day-to-day schedules
- Reporters frequently use a mix of personal and corporate accounts
Let’s look at 2 use cases
Securing @nytimes on Twitter

- Consider ways in which this account could be hacked
  - Including the classification and capabilities of adversaries
- Initial steps: strong, unique password and two-factor auth
- Limit or eliminate the use of third-party integrations
- Policy for how and when the account is used, even for DMs
- Build a relationship with Twitter for urgent assistance
Communicating with a source

- Consider ways in which the source could be compromised
  - Including the classification and capabilities of adversaries
- Reporter and source have different levels of tech comfort / knowledge
- You have to consider the lowest common denominator
- Policy must follow industry best practice, not something custom
- Educate the newsroom, educate future and current sources
Online threats and harassment

- Online threats aren’t new, but have escalated and are different
- A challenge we share with other media orgs
- Provide mechanism to report, create structure to triage
- Digital, physical, emotional support, build a resilient newsroom
- Take proactive steps prior to research and publication
Other things we’ve done

- Regular phishing assessments, sometimes targeted, always educational
- Security awareness training for new hires, tailored training w/desks
- Awareness through newsletters, weekly tips, advisories + NCSAM
- Believe culture must be part of the security program
- Build relationships with external vendors and teams
How can we empower other media orgs?
Securing all newsrooms

- Share experiences, intelligence, lessons learned
- Supporting users with personal/corporate accounts is tricky
- How can newsrooms securely use Twitter, Facebook?
- Not everyone’s got personal/professional contacts
- Can we work together on online threats/harassment?
Thank You!