NABA Cybersecurity Recommendations for Personnel both Enterprise and Operating in the Field

Working in the Enterprise

Personnel working in the enterprise should follow the recommendations of their employer's internal Information Security/Cybersecurity team. These will likely include the following baseline recommendations:

- Ensure your laptop has antivirus, antimalware, or endpoint malware detection tool installed and that it is kept up to date;

- Employ a password manager to generate and store strong, complex, unique passwords;
    - Your employer may provide access to a password manager.
    - LastPass, 1Password, Keepass, and Password Safe are all examples of popular and trusted password managers for enterprise and personal use.

- Enable multi-factor authentication (MFA) for all accounts;
    - Use a code generator application like Google Authenticator, Microsoft Authenticator, or Duo wherever possible.
    - Receiving two-factor codes via text message is also better than only having a single factor for authentication but is subject to some security risks.

- Employ only licensed software and check with IT teams before deploying unknown or untrusted software tools;

- Your company's IT teams should make software and computer updates available to you on a regular basis.
    - When these become available, promptly download and install all software patches.

Operating in the Field

Journalists working in the field are often focused on covering the story rather than digital security and safety. However, adversaries all over the world are targeting journalists with more intensity, aggression, and sophistication all the time.

Threat modeling is important, specifically in advance of working in the field. This is a simple process for considering what threats may present themselves while working in the field, how likely they are to manifest, and what steps you can take to counter the risks.

Beyond threat modeling, there are a handful of other key points to consider:

- If a journalist has access to a smartphone and/or laptop that can be used specifically for travel, this can help address the above issue. Traveling with a device that has minimal usage and data stored on it can reduce the risks to that data while operating in risky areas;

- When traveling domestically or internationally, reporters should always strive to keep their most essential electronic devices on their person whenever possible;
    - This means not leaving computers or phones in hotel rooms or as part of checked baggage when flying, taking trains, or buses.

- Sign out of applications that might store or transmit sensitive or confidential data before entering into higher-risk situations where authorities may compel a reporter to unlock and turn over a device for examination;
    - These applications include work and personal email clients, encrypted messaging applications like Signal or Telegram, cloud storage applications like Dropbox or OneDrive.
    - These situations include border crossings, interactions with law enforcement, clearing customs at airports, or when working in regions with significant police presence or police checkpoints.

- Consider powering off devices when they are not in use;
    - A device that has been powered off takes full advantage of the encryption used to protect its storage.

- If conducting a confidential conversation or interview, journalists should consider a number of options to minimize risks. In some situations, the content of the interview may be what must be kept confidential, in others the very fact that a source is meeting with a reporter may be risky.

- Journalists should create a secure back-up for sensitive information;
    - The best solutions for these are ones that are supported and secured by enterprise security teams, but other methods are also available. For example, creating encrypted volumes for backups on external drives can be a sufficient substitute.

- Use e-mail encryption and encrypt attachments as well. While this process can be difficult for those without extensive technical experience, some services can make it easier;
    - Encrypted email platforms like Protonmail and Tutanota have positive reputations for respecting users' privacy and making end-to-end encrypted email easier.

    - The Mailvelope plugin for Google Chrome and Firefox makes it easier to use encrypted email with services like Gmail, but still requires a good bit of configuration to use effectively

- Preference should be given to secure, end-to-end encrypted messaging, voice, and video messaging when operating in regions with established surveillance regimes;
    - Some apps like Signal have provided significant assurances that they protect and respect users' privacy and security. Others like WhatsApp may provide strong encryption, but fewer privacy protections.

- Use VPN connections at all times when connecting through the Internet;
    - Preference should be given to VPN solutions provided by your employer as they are better protected against privacy intrusions.
    - Some commercial VPN solutions are also acceptable, but should be considered carefully as many are known to be abusive of their users' privacy and may be willing to share information about user activity with third parties.

- As a journalist, separate personal accounts and information from work accounts and ensure there are as few connections between the two as possible;
    - It is usually impossible to keep these categories fully separate, but it is important to consider how mixing behavior and data stored can increase risks around that information.
    - Additionally, it is important to keep in mind that attackers will target both personal and work accounts. Maximizing protections for both is still very important.

- Consider employing advanced protection services, such as those offered by Google's Advanced Protection Program, and others;
    - Google's Advanced Protection Program is an industry-leader in providing more robust protections for users' accounts. One of the most important elements is the hardware token for multifactor authentication.
    - However, the Advanced Protection Program and other similar programs do not provide protection from legal actions that may compel the service provider to turn over information from your account.

- Reporters and other staff working in the field should review and take advantage of the security guidance and planning resources provided by organizations like Citizen Lab's Security Planner (securityplanner.org), Totem (totem-project.org), Freedom of the Press Foundation (freedom.press), and Committee to Protect Journalists (cpj.org).

- When returning from a risky destination, all laptops, smartphones, and other devices should be wiped and restored before being connected to the enterprise network.

- For devices that show evidence of tampering, analysis should be performed to determine what may have taken place and whether the device should be demolished and recycled.

October 6, 2020