DIGITAL SAFETY TRAINING FOR UKRAINIAN JOURNALISTS AND CIVIL SOCIETY

SAFEGUARDS FOR THE ONGOING CONFLICT WITH RUSSIA

BY **NATALIA ANTONOVA**

IN PARTNERSHIP WITH THE INSTITUTE FOR SECURITY AND TECHNOLOGY

APRIL 6, 2022

IST Institute for SECURITY + TECHNOLOGY

SITUATION OVERVIEW

Russia's invasion of Ukraine is causing destruction, death, and instability, deeply disrupting Ukrainian society. The Kremlin and its operatives are actively utilizing intimidation, disinformation and propaganda, censorship, cyber attacks, and various other means to restrict and influence the movement of information throughout Ukraine, Russia, and the international community.

With such ongoing tactics, every Ukrainian citizen, journalist, advocate, and government official with access to potentially sensitive information—including those in contact with at-risk populations—should exercise heightened caution and discretion.

According to the United States and Western governments, Russia maintains lists of key people to capture and potentially kill on Ukrainian territory. This means that safeguarding key information is of utmost importance in resisting the Russian threat.

This guide intends to provide practical tips to safeguard your digital activities and improve your digital hygiene. For the purpose of this guide, we define *digital hygiene* as a set of regular practices to keep one's digital assets and footprint secure.

HOW TO DO DIGITAL TRIAGE IN TIME OF WAR

– ***Digital triage:*** *the assignment of urgency to all tasks associated with one's cyber hygiene.*

For additional resources, please see The Totem Project, the Committee to Protect Journalists, the PEN America Online Harassment FIeld Manual, and the Global Cyber Alliance Cybersecurity Tool Kit for Journalists.

1. TAKE CARE OF YOURSELF

- **Reduce panic.** Just as when facing a physical threat, panicking when facing a cyber or digital threat can be dangerous.
- **Practice "square breathing"** whenever necessary:
  - Inhale through your nose while counting slowly to four.
  - Hold your breath while counting slowly to four.
  - Exhale through your mouth while slowly counting to four.
  - At the bottom of your breath, hold it again while slowly counting to four. Repeat as necessary.

2. STRIKE A BALANCE BETWEEN VIGILANCE AND CALM WHENEVER POSSIBLE

- You may feel a duty to post public content during wartime. That's absolutely understandable! Just try to **be aware of the implications** of what you are posting, so you don't have to deal with nasty surprises.

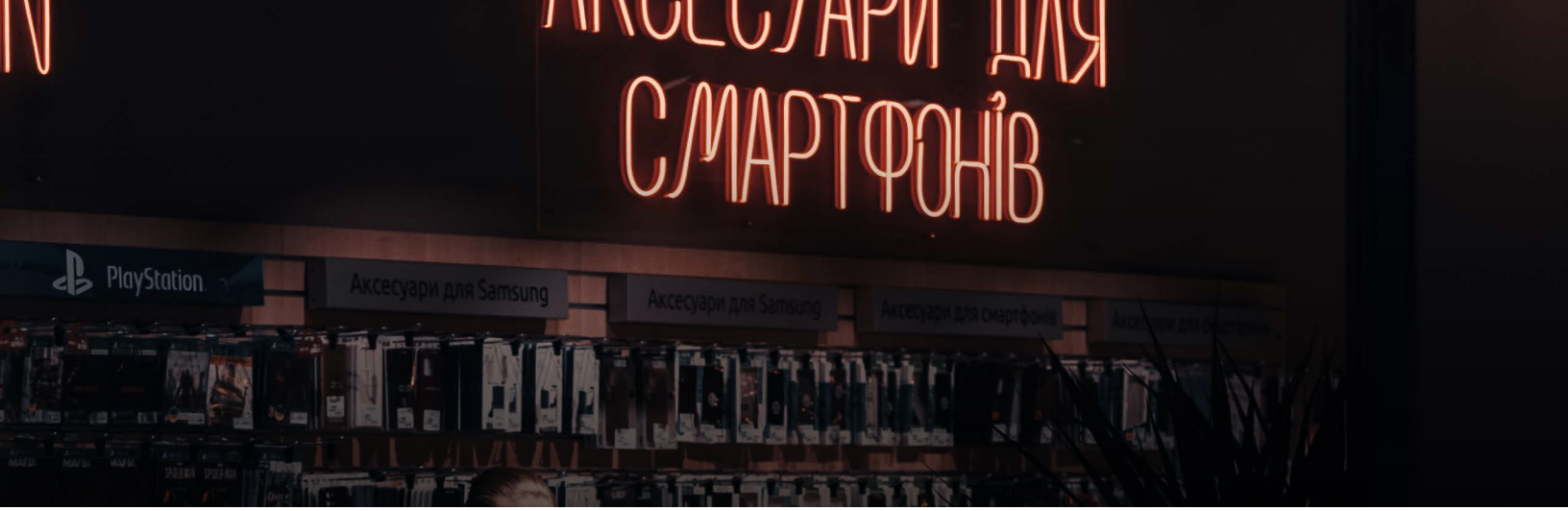
- We are all human beings, and hence we are all vulnerable in a variety of ways. Remember, your goal is not to be a superhero—it is to **sustain, and protect your data and the data of any vulnerable people** you are connected to.

- Remember also that there are no superheroes among the enemy either. **Don't give the enemy total control over your life**, no matter how much they try to terrify you.

- **Psychological warfare is a common tactic of war**. The enemy's goal is to have you stressed and constantly afraid. Resist such tactics whenever possible.

3. ASSESS THE STATE OF YOUR DATA

- Soberly and methodically, **assess your digital footprint and your digital attack surface**.
  - Your *digital footprint* includes all applications for which there is a unique user ID. This includes: public and private information online—including any document uploads, contact lists, databases (which can be highly porous), social media accounts, profiles on shopping and hobby sites, etc.
  - Your *attack surface* includes any potential entry points for malicious parties—including software, hardware, data storage, content with your name on it, content you are tagged in, and so on.
- **Identify the weakest links in your digital footprint.** Have you had a history of reusing passwords? Are you aware of any compromised databases you may be on? Have you shopped on compromised sites? How public are your social media posts and pictures?
- **Do not trust public wi-fi** to send, transmit-send, or receive sensitive information.



4. TAKE BASIC STEPS TO PROTECT YOUR DATA

- **Craft strong passwords** that no one can break. Use letters, numbers, capital letters, special characters, and phrases that are not easily recognizable.
  - Use a password manager. A simple password or browser tool can help you see any passwords associated with your e-mail accounts that are compromised or repeated. LastPass is one possibility.
  - For more information, visit Passwords for Journalism.
- **Turn on 2-factor authentication** for all of the accounts that offer the capability, including: social media and email accounts wherever possible. Do the same for bank accounts, utilities accounts, sites where you have done shopping, gaming platforms, etc.
- **Enroll in Gmail's** Advanced Protection Program.
  - This requires a physical security key, like Google Titan or a Yubikey, but offers greater protection beyond 2-factor authentication.
- **Make sure all of your software is patched and up to date**, and use anti-virus software.
- **If you are using a router, make sure it is as secure as possible**. Older routers in particular have greater vulnerabilities. Cheap, used routers may have backdoors installed by Russian intelligence—and we have seen many examples of this happening in Ukrainian institutions over the years. Consider regularly unplugging the router for one minute to reset it.
- **Wipe any accounts associated with Russian-hosted sites** such as Odnoklassniki and VKontakte, and make sure you are not reusing passwords from any of those sites and that your friend lists are not visible, as they can be potentially be used as an entry point to track at risk populations.

- ☐ **Make your friend lists private** wherever possible.
  - Go through your friend lists and remove anyone you don't know and/or anyone engaging in suspicious behavior.
- ☐ **Consider dropping the use of face ID** on your devices. It can easily be fooled.
- ☐ **Use a VPN**, particularly if accessing any Russian sites.
  - Use a protective DNS to prevent your computers and devices from connecting to known malware or phishing sites.
- ☐ **Turn off location tracking** on your devices and social media accounts.
- ☐ **Do not click on any suspicious links** and double check messages and e-mails if you are not sure as to their origin.
  - Remember that phone numbers can easily be spoofed. Do not click on strange/unexpected links, even if they come from someone you trust.
  - Instead, ask them, "Was it you who wrote that message?"
  - Watch out for "SIM Jacking."
- ☐ **Review and update social media privacy settings**.
  - Consider making most of your social media accounts private.
  - A second, public account is ideal for sharing news and videos without compromising your information.
- ☐ Only pass on important / sensitive information on **peer-to-peer encrypted channels**.
  - Do not use Twitter or Facebook DMs, or anything similar.
  - Do not use walkie-talkies to pass on sensitive information.
- ☐ **Add a PIN option to all of your encrypted chat apps**. You will be periodically prompted to enter this PIN.
  - WhatsApp, Signal, and Telegram all support adding a PIN.
- ☐ **Routinely fully shut your phone down** and then start it back up again after keeping it off for at least a minute.
- ☐ **Keep backups of your data**, and enable automatic backups to an external drive, not connected to your device.

5. CHOOSE WHICH CONTENT TO POST WISELY

- **Be smart about what you share**. In times of war, it is important to get information out about atrocities and other newsworthy events. However, consider that you may be sharing compromising information as well.

- **Always ask about tagging someone/identifying someone in a public post**. In peacetime, it's simply common courtesy. In wartime, it can save lives.

- Remember that even a random photo or video can be **geolocated** quickly.
  - To avoid being geolocated, do not share pictures in front of, or from the windows of your home or other places you frequent.
  - If you would still like to post content like this, consider doing it only on a private account or on an alternate, public account.

- If sharing **military-related content**, make sure to not reveal Ukrainian troop movements.
  - Blur out key details such as faces and/or license plates when possible, and military patches when applicable.
  - Special Forces, especially, must not be identified, as they are prime targets.
  - Simply delaying posting can help foil targeting of such forces, as well.

6. TAKE PRACTICAL PRECAUTIONS

- **Be observant of your surroundings**. If you worry that you may be under surveillance at home, leave a tiny bit of thread on your doorstep or a small speck of fluff on top of your laptop. These seemingly arcane tricks can be helpful when identifying surveillance, and won't give you away like a web camera might.

- If you are traveling across hostile territory, **consider bringing as many devices as possible**. The truth is: Any regular soldier at a checkpoint is likely not going to want to go through all of your belongings.

- **Change the names of important contacts in your system**. Are you in touch with the mayor of your city? Consider listing him as "Plumber Petro" instead of "Mayor Petro." It's a simple trick that can save a life.

- **Be wary as to whom you give your phone number**. Technology that can compromise you if someone has your number—even without action on your side—already exists.

- **Be aware of your surroundings**. It's a cliché, but the walls have ears—during war time, especially so.

- **Always pack your bags yourself**. Remember that tracking devices, even innocent-seeming ones such as AirTags, can be modified and easily used by nefarious individuals.

7. KEEP UP WITH EMERGING THREATS

- Make sure to keep abreast of **enemy troop movements** in your area.
- Please understand that even locations held by Ukrainians/locations in the EU and beyond have been penetrated by Russian intelligence. **Do not completely let your guard down**, even when seemingly surrounded by friendlies.
- **Be cautious about making new friends and acquaintances** during wartime and try to be aware of any unusual activities in your area.
- Do your best to keep abreast of **Russian disinformation tactics**.
- Are you sure your news updates are coming from reputable and verifiable websites and data sources? **Establish a list of websites, contacts, and accounts that you trust**, and be wary of impersonator accounts, trolls, and bots.
- **Be wary of sensationalized headlines**, and “think before you click.” In other words, think critically about the origin of information that you consume and share with your network.

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

counterdisinfo@securityandtechnology.org