



Cybersecurity Life “Hacks”

Sean Eyre
Ericius Security

\$> whoami

Sean Eyre

Christian, Husband

Founder, CEO of Erius Security

West Point, Computer Science

Former Army intelligence

Former Army defensive cyber

Judoka, Runner, doodler, OSINTer, Pythonista



Who are we?

- Erius Security exists to provide cybersecurity support to people serving in dangerous situations so that they can keep their people, information, and networks safe
- Cybersecurity professional services since 2018
- Risk assessments (What is my quest?)
- vCISO (How do I get there?)



Agenda

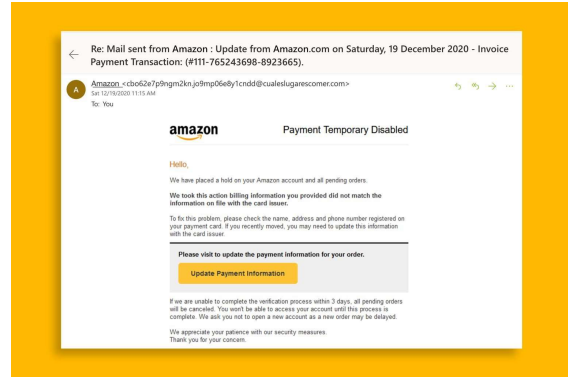
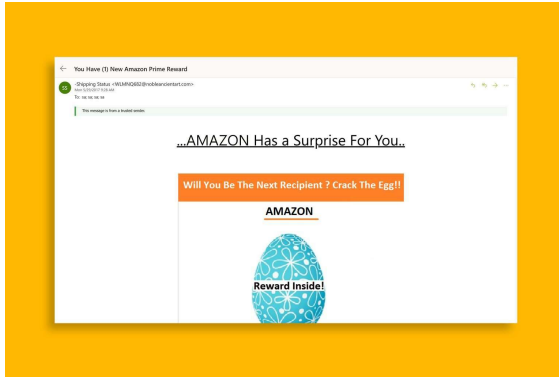
- Why Cybersecurity?
- Cyber Attack Impacts
- Personal Cybersecurity
- Common Secure Communications Tools



Why
cybersecurity?

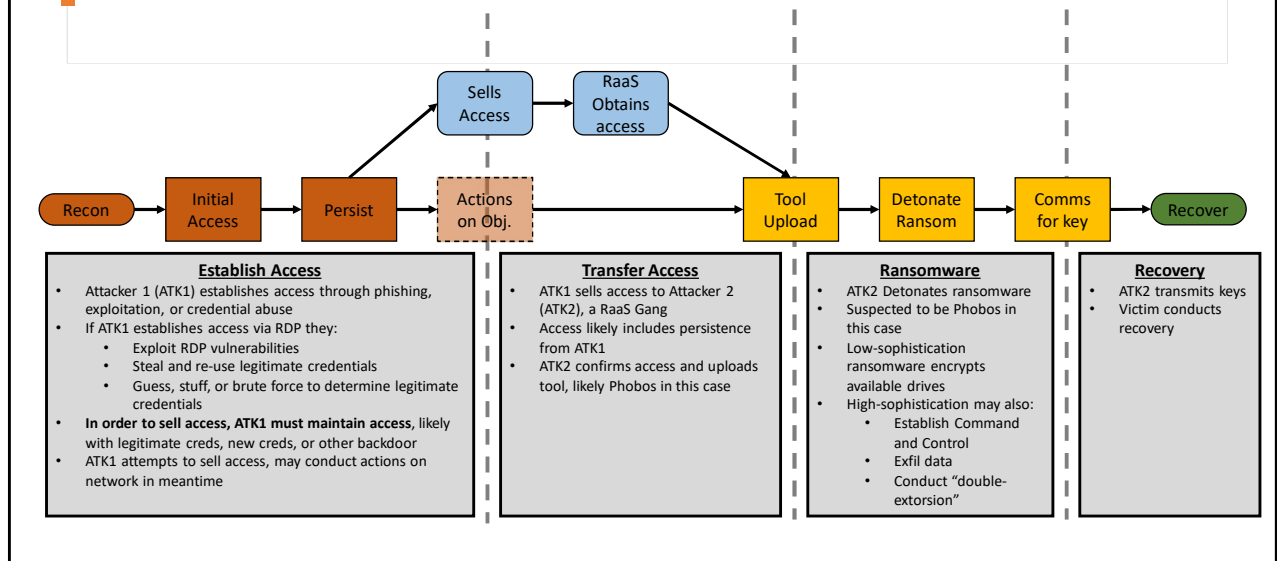


Phishing



<https://www.rd.com/article/amazon-email-scam/>

Ransomware as a Service



No money? No Problem! Ransomware has a price that fits your budget

Example based on Phobos TTPs

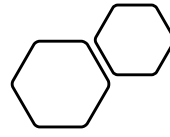
Two take aways:

ATK1 makes money by selling access to other attackers

ATK2 will buy access if it makes business sense for them

ATK1 might maintain access after the ransomware is removed

Cyber attacks
do not
recognize
borders



There is no “safe haven”

NGOs are increasingly
targetted

<https://blogs.microsoft.com/on-the-issues/2021/10/21/cyber-defenses-security-program-nonprofits/>

Valid targets are valid targets, at home, abroad, or both



Once upon a
springtime...

You have missionaries in an Eastern European country

A major world power escalates aggressive actions towards that country

Several news agencies go down with ransomware

The country is invaded

The power grid goes down due to malware

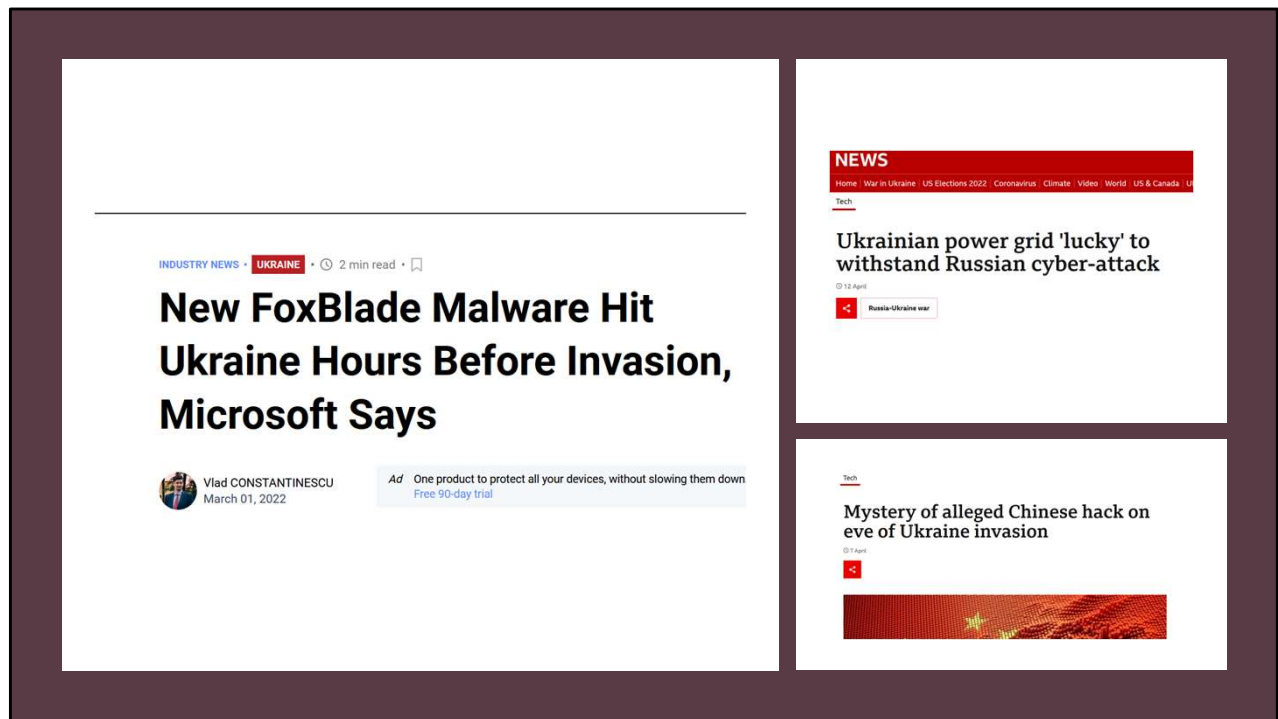
Fighting is fierce; Multinational companies are targeted with ransomware *to hinder their communications*

As the war continues towards winter, novel malware hits multinational logistics and transportation companies in the area

February 24th, the day before the invasion, FoxBlade/HermeticWiper targets various companies - <https://www.malwarebytes.com/blog/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine>

In April, Industroyer2 targets power grids-
<https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>

In October, Prestige overlaps with HermeticWiper, targets international logistics -
<https://www.reuters.com/technology/microsoft-says-ukraine-poland-targeted-with-novel-ransomware-attack-2022-10-14/>



Chinese actions - <https://www.bbc.com/news/technology-60983346>

Ukrainian Powergrid - <https://www.bbc.com/news/technology-61085480>

FoxBlade vs Ukraine - <https://www.bitdefender.com/blog/hotforsecurity/new-foxblade-malware-hit-ukraine-hours-before-invasion-microsoft-says/>

Your foreign
office is hit
with
ransomware...


It rides the connection home to
the States...

It's HermiticWiper...

How do you
do crisis
comms in
this
situation?

*What is the human
impact?*

Your **organization** needs a plan for this



Agency wide
cybersecurity starts
with personal discipline

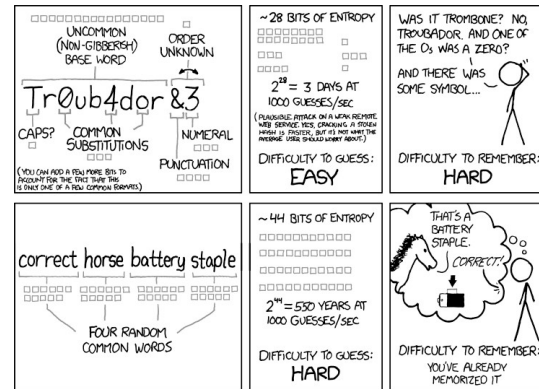
1. Multi Factor Authentication

- Put MFA on everything you can
 - *The single biggest ROI for the effort involved*
 - Severe hinderance to phishing and unauthorized access
 - One-time Passcodes and push notifications are great
 - Hardware keys (Yubikey, etc) are best, but inconvenient
 - SMS is okay if it's what you have

Authy
Google Auth
Microsoft Auth
Duo for paid

2. Strong passwords in a manager

- Long passwords are good – 5 random words
 - DO NOT use biometric log in
- Use password managers like KeyPassXC, BitWarden, or Keeper
 - Cloud vs Offline



<https://xkcd.com/936/>

3. Anti-malware

- Choose an anti-virus/anti-malware solution and keep it up to date
 - Defender is fine
 - Malwarebytes is fine
 - Organizational/Paid EDR is better
- Let it auto-update and auto-scan
- Let it block malware and notify you

Defender is fine
Malwarebytes is fine

Paid, organizational EDR is better

4. Automatic updates

For your OS

For your software/applications



For the OS
For software

5. Secure Backups



SELECT AN OUT-OF-BAND
BACKUP SOLUTION



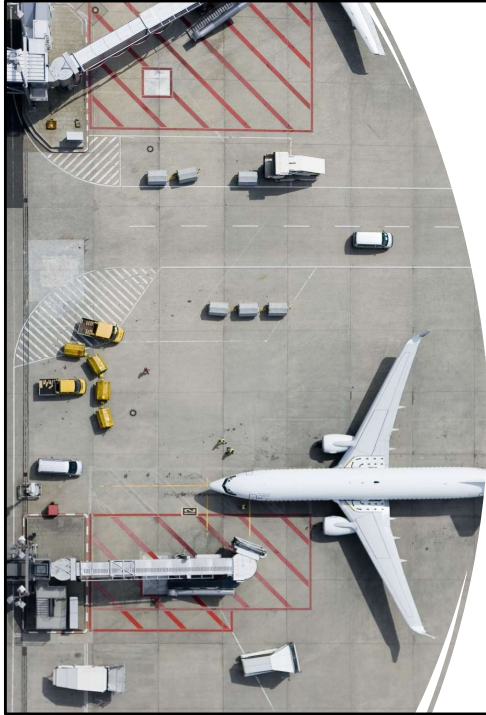
BACKUPS TO THE CLOUD



BACKUP BEFORE YOU
LEAVE

Not OneDrive or Google Drive synch (these can replicated problems into your cloud store and are **availability, sharing, and collaboration solutions** not backups)

Use something like Carbonite to replicate individual files and restore from safe versions



Accessing Org Accounts While Traveling

- Keep it in the cloud (if internet access won't be an issue)
 - Don't synch cloud drives, email, etc
- Access it via Incognito Browser and use your password manager
- Close the browser when complete

Secure Messengers: Security Features

Essential:

- E2EE and other encryption, preferably with keys under your control
 - Forward Secrecy
 - Zero Knowledge
- Contact verification
- Support for MFA
- Design/architecture documented
- Independently Audited, open about problems

Useful features:

- Disappearing messages
- Registration without phone/email



Security Messengers: Best in Breed

- **Signal**
 - Top tier, non-profit funded
 - Uses phone numbers (e.g. privacy and security, not anonymity)
- **Threema**
 - Paid, independent Swiss company
 - No contact information needed to register

	Threema	Signal	Telegram	WhatsApp
E2E Encrypted Messages	✓	✓	✓	✓
Disappearing Messages	✓	✓	✓	✓
Group Messaging with User Permissions	✓	✓	✓	✓
Encrypted Voice Calls	✓	✓	✓	✓
Anonymous (does not require phone number)	✓	✗	✗	✗
Ability to Bypass Country Blocks	✗	✓	✗	✗
Does NOT collect metadata (phone number, GPS, timestamps)	✓	✓	✓	✗
Does NOT collect phone contacts	✓	✓	✓	✗
Open Source Client Software	✓	✓	✓	✗
Third-party Source Code Audits	✓	✓	✗	✗
Decentralized Message Storage	✓	✓	✗	✓
Free	✗	✓	✓	✓
Financing	One time purchase	Non-Profit	Private Russian Investors	Advertising
Jurisdiction	Switzerland	USA	Dubai	USA

- <https://akana.ch/en/it-consulting/it-security-en/how-whatsapp-threema-signal-and-telegramdiffer-in-terms-of-data-protection-and-security-an-analysis/>
- <https://utopia.fans/tools/the-best-chatting-messenger-threema-vs-signal-vs-utopia/>

VPNs

- **Virtual Private Networks**
- VPNs establish secure and encrypted connections to provide you online privacy and anonymity
- How to select the best VPN plan:
 - **Transparency:** Has a clear privacy policy and transparency report
 - **Price:** Should provide info on what the cost covers
 - **Audits:** External audits are publicly available



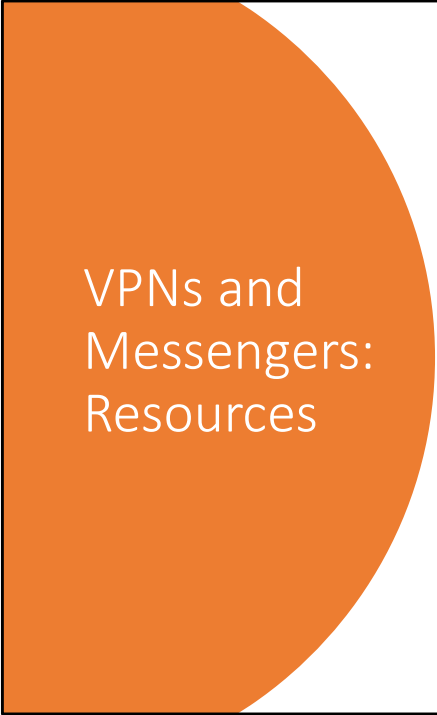
Point 1: VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. This prevents people, websites, and governments from tracing your online activity back to your computer. (Norton, 2020)

Point 2:

- **Transparency** is the most important criteria. Your VPN should have a clear privacy policy that contains a commitment to never collect or share logs. They should also have a recent transparency report that describes the data they collect on you
- **Price:** You should pay for any quality VPN that you use. This is not an area you want to skimp on. The cheaper it is, the less reliable it likely is.
- **Audits:** This is the least important criteria. The best VPNs have hired external auditors to review their code, test their servers, and find unknown vulnerabilities. If available, your VPN provider should disclose what audits it has requested and the results.

Transition: In your workbook there was a pre-class exercise for those of you that have a VPN. Next we'll break into groups and discuss what we came

across in our research.



VPNs and Messengers: Resources

- <https://restoreprivacy.com/>
- <https://ssd EFF.org/en>







Laptops

- Separate admins
 - UAC is on
- Anti-virus
 - MalwareBytes or Windows Defender
 - MalwareBytes AdwCleaner
- Auto-updates for OS, Software, and BIOS
- Review your software and remove unused applications
- Turn off NFC/Bluetooth
 - Always use wired devices in security sensitive situations
 - Prevents BlueJacking and BlueSnarfing
- Avoid public WiFi when possible in favor of encrypted WiFi
- Use a VPN when on untrustworthy networks like public WiFi (see WiFi section)



Laptops

- Lock down your browser
 - Block Trackers with a tool like Privacy Badger
 - Close all sessions/logout when browser closes
 - Install an Ad blocker
 - Don't use the browser's password manager
- Firewall
 - Set WiFi/Network Profile to public on Windows 10 to make the computer "not discoverable" by default
 - Set the firewall to reject all in-bound connections

<https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c>

Laptops

- Create backups
 - Copy sensitive files off to a USB drive routinely
 - Create system restore points routinely
 - Enable Volume Shadow copy
 - Create a full backup/use a backup service – **At least one recent backup needs to be disconnected from your network**
 - Consider a service like Carbonite or even OneDrive/GoogleDrive
- If your organization has mobile device management (e.g. MSFT Intune), enable remote wipe
- Full Disk Encryption using VeraCrypt or BitLocker (Windows)

<https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c>

Cell Phones

- Never root the phone
- Encrypt the phone's hard drive and any SD card
- Lock the SIM with a PIN – Put it in a password manager
- Lock the phone with a long PIN/Password
 - 6+ characters
 - DO NOT use biometric log-ins
- Set up auto-lock to 30 seconds or less
- Minimize apps installed
- Only install from Official Stores
- Updates:
 - Update before you leave
 - If you're only gone for a few days, disable auto-updates
 - Auto-update from a trustworthy location
 - Manually update OS as necessary

Explain Rooting



https://media.defense.gov/2021/Sep/16/2002855921/-1/-
1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF



Cell Phones

- Routinely check your privacy settings – OS updates may change them
- When charging your phone
 - Never use public USB ports
 - Bring your own power block (charger) or external battery
- Enable Remote Wipe
- Disable Location Services. Enable only for specific services/specific use



Cell Phones

- WiFi off when not in use;
 - Disable automatic WiFi connections
 - Consider an always on VPN if legal where you live/are traveling
 - Setup VPN as always on/automatically use if on public networks
 - Forget WiFi networks frequently
- Bluetooth only when essential
- Disable “access from lock screen” for digital assistants
- Periodically review app permissions for concerns



Cell Phones

- Avoid sensitive conversations over regular cell or regular text
- Do not open links sent via text or email unless you recognize the sender AND are expecting it
 - If you can, delete the text or email without opening it
- If a strange pop-up appears, close all applications immediately rather than click on it

WHAT CAN I DO TO PREVENT/MITIGATE?													
THREAT/VULNERABILITY	Update Software & Apps	Only Install Apps from Official Stores	Turn Off Cellular, WiFi, Bluetooth	Do Not Connect to Public Networks	Use Encrypted Voice/ Text/Data Apps	Do Not Click Links or Open Attachments	Turn Device Off & On Weekly	Use Mic-Drowning Case, Cover Camera	Avoid Carrying Device/No Sensitive Conversations Around Device	Lock Device with PIN	Maintain Physical Control of Device	Use Trusted Accessories	Turn Off Location Services
	Spearphishing (To install Malware)												
	Malicious Apps												
	Zero-Click Exploits												
	Malicious Wi-Fi Network/Close Access Network Attack												
	Foreign Lawful Intercept/ Untrusted Cellular Network												
	Room Audio/ Video Collection												
	Call/Text/Data Collection Over Network												
	Geolocation of Device												
	Close Access Physical Attacks												
	Supply Chain Attacks												
<div><div>Does not prevent (no icon)</div><div> Sometimes prevents</div><div> Almost always prevents</div></div>													

https://media.defense.gov/2021/Sep/16/2002855921/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF