



Digital Safety: A Layered Defense for Researchers & Advocates

Key Principles from Bellingcat's
Investigative Tech Team

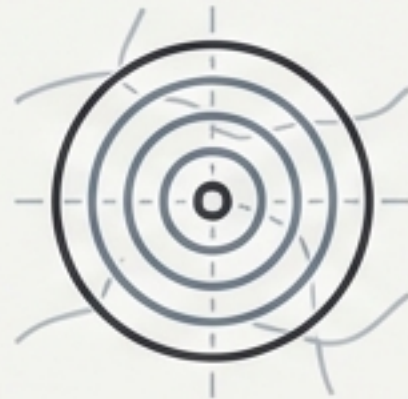
Your Security is Personal, Not One-Size-Fits-All

Every researcher, journalist, or advocate faces different risks depending on their work, location, and online profile. The first step is to understand your unique threat landscape. This strategic exercise is called **Threat Modeling**.



1. Identify Adversaries

Who might target you?



2. Map Risks

What are the consequences of exposure? (e.g., surveillance, phishing)



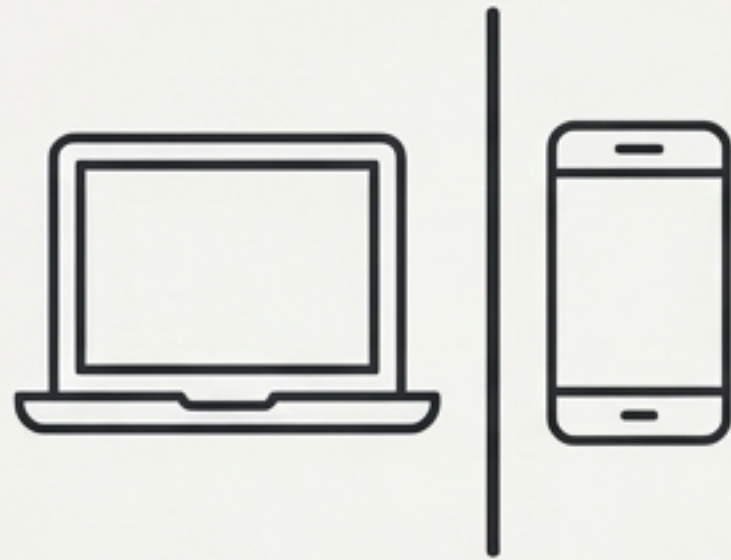
3. Plan Mitigations

How can you counter these specific risks?

*It's important not to get paranoid.
The goal is insight, not fear.*

The First Defensive Line: Separate & Fortify Your Digital Identities

For sensitive research, creating a strong boundary between your professional and personal life is critical. This separation protects your work, your sources, and your mental hygiene.



Use separate devices for sensitive assignments



Create accounts not linked to your real name or profiles



Use separate SIM cards

Beyond Passwords: The Power of Passphrases & Managers

A good password is the first lock on your digital gate. The three rules are simple: **Long, Complex, and Unique** for every single account.

Bad

P@ssw0rd1! ✗
(Predictable)

Passphrases

correct + horse + battery + staple

Good

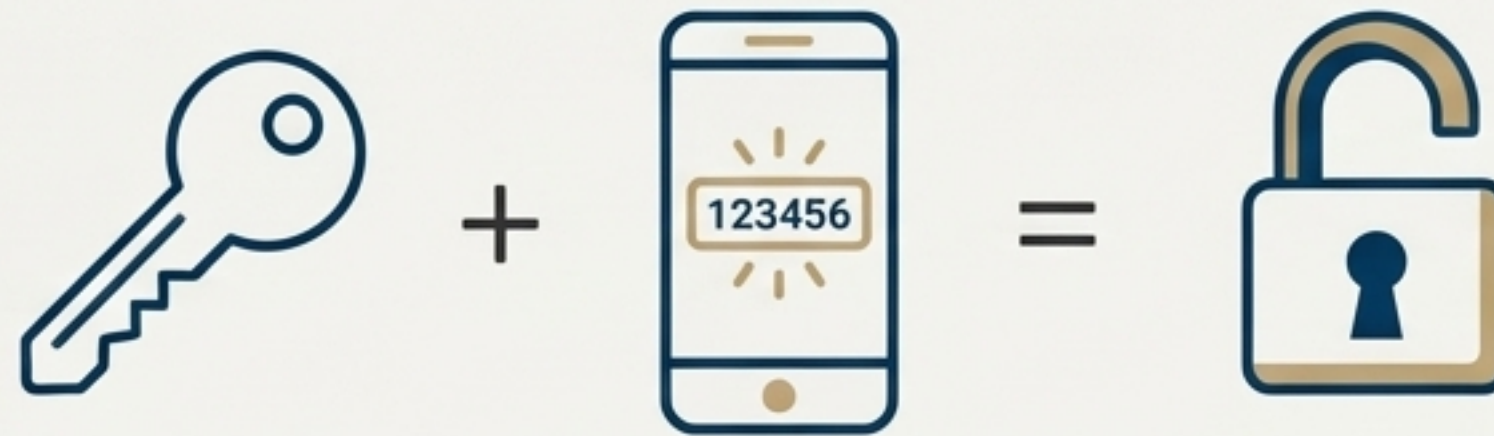
kR8\$v!2zP#n@5qW9&eB* ✓

Instead of complex strings, use **passphrases**. Combine multiple random words to create a long, memorable, and secure password.

It's impossible to remember them all. The single most important step is to use a **Password Manager** to securely store and generate unique passwords for every account.

The Digital Double-Lock: Enabling Two-Factor Authentication (2FA)

2FA adds a critical second layer of security to your most important accounts (email, financial, work platforms). It combines your password with something external to the device you are logging in on.



[Your Password] + [External Code] = Access Granted.



Authentication App

An app on your phone generates a time-sensitive code. (Examples: Google Authenticator, Authy).

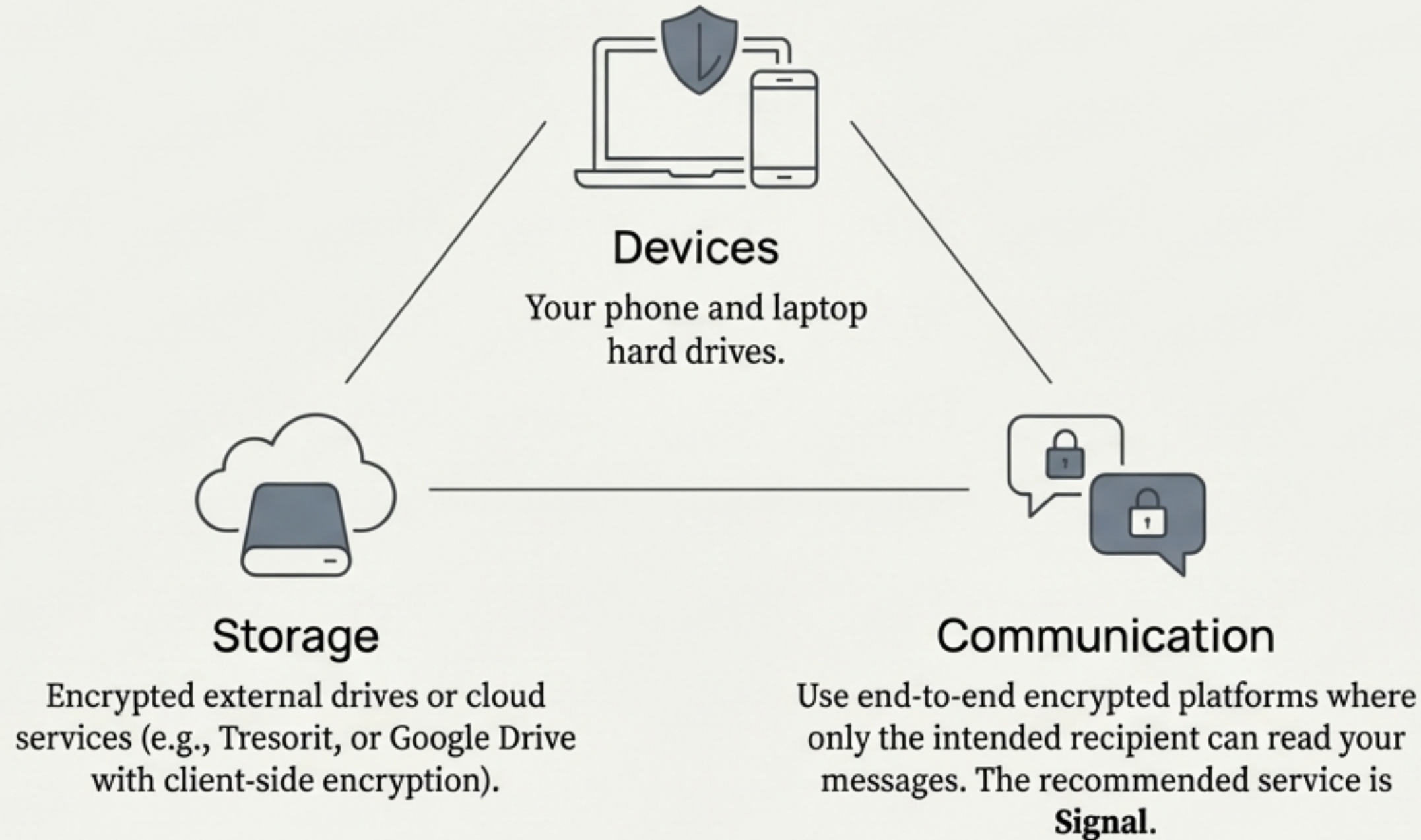


Physical Security Key

The most secure method. A small electronic key you plug into your device to verify your identity.

The Unbreakable Vault: Encrypt Everything

If your device is lost or stolen, encryption is what prevents an adversary from accessing your data. It should be applied across your entire digital ecosystem.



The Remote Kill-Switch: Prepare for Loss or Theft

Most devices have built-in tools that allow you to take action if your device is compromised. The key is to set these up in advance so you are ready to respond in an emergency.

Android: **Find My Device**
Apple: **Find My**



LOCATE

See your device's last known location.



LOCK

Remotely lock the screen to prevent access.



ERASE

Remotely wipe all personal data from the device.

Check that these tools are enabled and updated on your devices now.

Fortifying Your Base: Your Home Wi-Fi Network

Even your home network requires fortification. Follow this checklist to secure it against unauthorized access.



1. Change Default Credentials: Update the router's default admin username and password.



2. Use a Strong Password: Set a long, complex, and unique password for the Wi-Fi network itself.



3. Disable WPS: Wi-Fi Protected Setup is a known security vulnerability that can be exploited.



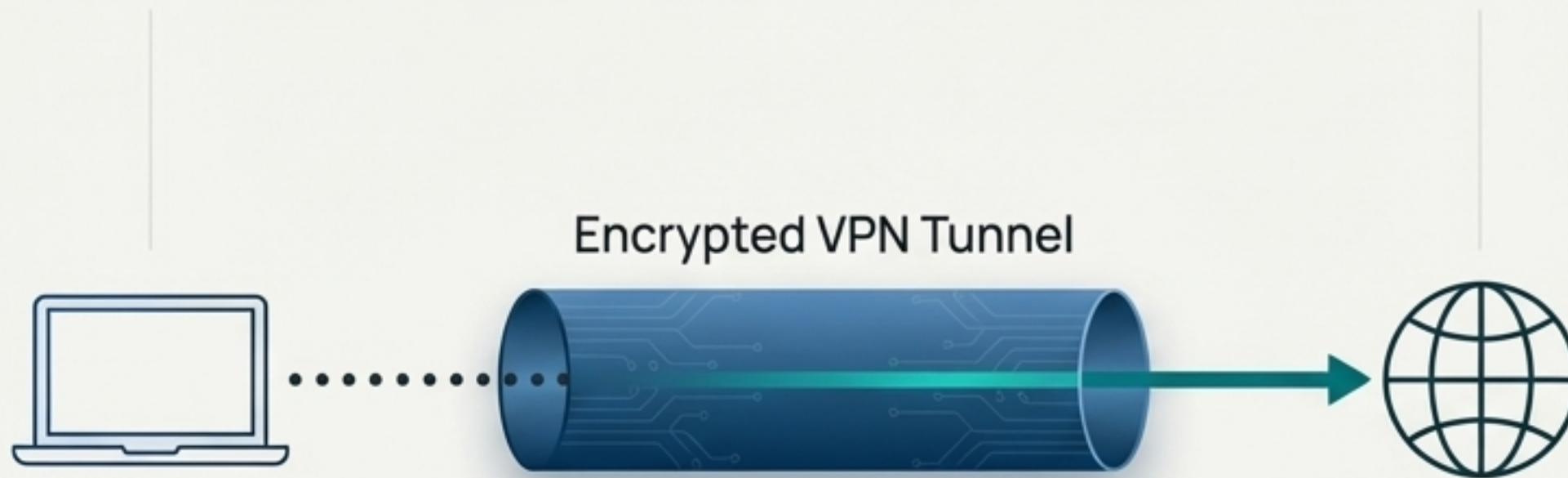
4. Enable MAC Address Filtering: Restrict network access to only your authorized devices.



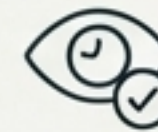
5. Use WPA3 Encryption: If buying a new router, ensure it supports the latest and most secure standard.

The Invisibility Cloak: Using a Virtual Private Network (VPN)

A VPN protects your internet traffic by routing it through a secure third-party server. This hides your IP address and encrypts your activity, shielding it from your internet provider or hackers on public Wi-Fi.



How to Choose a Trusted VPN



Transparency: Is it open about its encryption levels and security features?



Reviews: Does it have a strong, verifiable reputation?



Jurisdiction: Crucially, ensure it is **not based in a Five Eyes country**, where companies can be compelled to share user data.

A VPN is not a magic shield. It won't protect you from malware, phishing, or bad security habits.

Safe Passage: Hardening Your Web Browser

Your browser can be a major vulnerability or a powerful tool for privacy. Take these steps to secure it.



Choose a Privacy-Focused Browser

Start with a browser built for privacy, such as **Firefox** or **Brave**.



Adjust Your Settings

Enable features like **HTTPS-Only Mode** and other safe browsing settings recommended for your browser.



Install Trusted Extensions

Add extensions that block ads and trackers, such as **uBlock Origin** and **Privacy Badger**.

Regularly clear your cookies and site data to prevent sites from tracking your online activity.

Patching the Armor: The Critical Role of Updates



Updates aren't just for new features. Their most important function is to **patch security vulnerabilities** discovered in your software (OS, browser, VPN, antivirus, etc.).

Enable automatic updating whenever possible.

Make it easy for yourself.

For advanced threat models, you might consider delaying automatic updates by a week or two. This can help avoid any unexpected side effects or bugs introduced by a new update.

The Digital Immune System: Antivirus Software

Trusted antivirus software acts as a protective layer between your device and external threats. It scans files and programs for malicious code, blocks suspicious activity, and prevents the spread of malware and ransomware.



Built-in

Check the default service your OS provides and evaluate its effectiveness.

Free Solutions

Offer basic, foundational protection.

Paid Solutions

Required for real-time monitoring, advanced threat detection, and robust phishing protection.

Recognizing the Enemy: Spotting Phishing Attacks

Even with perfect technical security, you are still at risk from attacks that trick you into revealing sensitive information. Always think before you click.

Phishing Red Flags Checklist



Urgency: Language that demands “immediate action.”



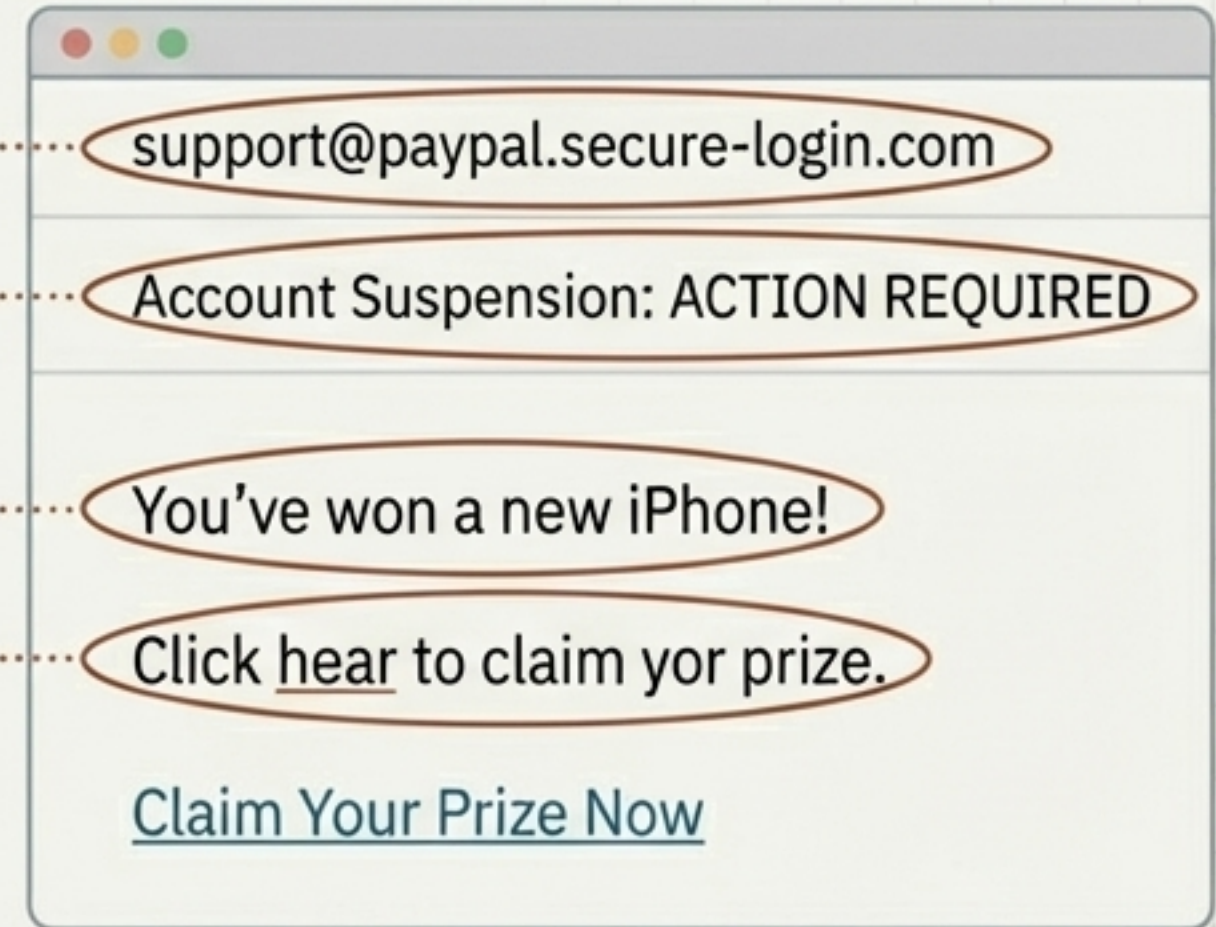
Unbelievable Offers: Something that is ‘too good to be true.’



Errors: Obvious spelling and grammar mistakes.



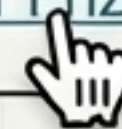
Sender Mismatch: The sender’s email address doesn’t match the company they claim to be.



Pro-Tip: Hover, don’t click. Move your cursor over any link to see the the true destination URL before you click on it.

http://bit.ly/malicious-link-123 or
http://www.evildomain.com/login

[Claim Your Prize Now](#)



Your Greatest Tool is Awareness

“With phishing, it becomes clear that awareness is the most important part of digital safety.”

Technology provides the walls, the locks, and the armor.
But you are the guardian on the wall. Your vigilance is the final, and most critical, layer of defense.

Digital Safety is a Process, Not a Destination

Threats evolve, and the tools to protect yourself develop quickly.
Staying informed is part of staying secure.

Continue the Conversation.



Join the ongoing discussion about digital safety in the **Bellingcat Discord server**. In the **#infos** channel, you'll find more tips, community support, and specific program recommendations to help you upgrade your security measures.

