Dear community members,

The recent $53 million hack of Radiant Capital through compromised signatory devices shows just how important good security practices are in the crypto space - even sophisticated users can fall victim to attacks. Whether you're managing a significant amount or influence over cryptographic assets, having a solid security setup for your devices and software is essential to protect your assets. This guide walks you through practical security measures that will help shield you from threats while keeping your crypto accessible when you need it.

Practical Security Measures

The Dedicated Computer Setup

Having a separate computer for onchain transactions creates a clean, controlled environment. Every website you visit and email you open on a regular computer creates potential exposure to malware. By maintaining a dedicated system, you're drastically reducing your attack surface. This computer should be treated like a specialized tool - it has one job, and it does it securely. If this is not possible, other solutions such as virtualisation are viable, and while they offer an increased layer of security, they are not as secure as a dedicated system.

Software Hygiene

Good software practices form your foundation for secure transactions. Downloading from official sources and verifying checksums validates your tools haven't been compromised. While updating software and running antivirus might seem basic, they're crucial first-line defenses against known threats. Disabling unnecessary services isn't just good practice - it eliminates potential vulnerabilities that attackers could exploit. For example, recently a Nation State sponsored attack was detected and eventually stopped by simple antivirus after the company hired an IT manager who was actually working for North Korea.

Storage Device Safety

Hardware wallets are secure by design, but their security depends heavily on how you use them. Every USB connection is a potential attack vector, so it's essential to maintain strict control over what devices connect to your computer for onchain transactions. Keeping WiFi disabled by default isn't paranoia - it's a practical way to minimize network exposure when you're not actively trading. While it is not practical if you do not have a separate system for signing, then not keeping your hardware wallet permanently connected would be the next best defense.

Basic Device Protection

Full disk encryption, strong authentication, and automatic screen locks are fundamental security measures that protect against both opportunistic and targeted attacks. Regular encrypted backups (excluding seed phrases) enable you to recover from hardware failures without compromising security. These basics might seem obvious, but they're often the difference between a failed attack and a catastrophic loss. Storing your seed phrases on the computer you use with the wallet is also not a good idea because if that computer is compromised, so is the wallet.

Network Security

Your home network needs to be treated as part of your security perimeter. Using public WiFi for transactions is an unnecessary risk - the potential convenience isn't worth the exposure. A reputable VPN adds another layer of privacy and security, while keeping your router updated and patched for known vulnerabilities. These aren't just best practices - they're essential tools for maintaining transaction privacy and security.

Remember: security is about layers. Each measure might not be perfect on its own, but together they create significant barriers to attack. Good security should be thorough but not paralyzing - the goal is to protect your assets while still being able to use them effectively.

North Korea as an Example of a Potential Threat Actor

Certain jurisdictions, such as North Korea, are known for having established cyber programs that, in some cases, are aimed at raising funds for their respective regimes. For instance, North Korea has been linked to financially motivated cyber activities for years, with an increasing focus on the crypto sector. Monitoring the tactics associated with these actors can be prudent, as they may employ various techniques, including fake job recruitment scams. These scams often target roles within tech and crypto industries. To mitigate such risks, consider implementing the following essential steps:

Authenticate Recruiters and Employers

Always verify a recruiter's profile on LinkedIn or through the official company website. Some recruitment scams even mimic real companies like Meta and Samsung, so verify by calling the company directly using contact information from their official site—not from the recruiter's email. Keep in mind that who you see on a web conference is sometimes not the person who you are talking to. Modern AI can render video based on written or real time dialogue. Look for lag on the other person's lips or jerky motion / artifacts. You can also use an external background check company (like Zinc) if you are the party doing the hiring.

Avoid Downloading Unknown Files

Be cautious about downloading any software or files as part of an interview process. Hackers frequently use malware disguised as job-related materials, such as PDFs or video conferencing apps that don't function as expected. Google has identified these tactics, noting that such files often appear malformed or corrupted. Most applications have a way of controlling if they download files automatically from their settings but by default, these messaging apps typically have auto-download settings enabled:

- Google Messages (automatically downloads files up to 100 MB over mobile data by default)
- Samsung Messages (automatically downloads MMS content)
- WhatsApp (media auto-download is usually on by default for photos and other files over Wi-Fi)
- Signal and Telegram allow fine-grained control, but they generally do not enable auto-download for all file types by default; users are prompted to set these preferences manually.

Be Wary of Excessively Remote Positions

Many scams target remote job seekers, which makes it harder to validate the recruiter's legitimacy. If a position requires relocating but the interviewer offers remote options right away, investigate further.

Conduct Direct Research

Look for official job postings through verified career portals like LinkedIn, Glassdoor, or company career pages, rather than relying solely on email offers. Cross-reference the job description on the company's official website to confirm its authenticity.

Be Cautious of Social Media Connections

Some threat actors have a history of impersonating recruiters on social media to lure candidates, often in the defense and cybersecurity fields. If contacted via social media, request an official email from the recruiter's company domain and research their social media history for inconsistencies.

Use Strong Cyber Hygiene

Use multi-factor authentication (MFA) on all critical accounts, especially those related to crypto wallets or financial platforms, as attackers often use social engineering to access sensitive accounts.

Final Thoughts

The crypto landscape continues to evolve, and with it, the sophistication of threats targeting digital assets. While the measures outlined in this guide may seem extensive, they represent a balanced approach between security and usability.

Key takeaways to remember:

- Maintain separation between crypto operations and daily computing activities
- Implement multiple layers of security rather than relying on a single measure
- Stay vigilant about North Korean recruitment schemes and social engineering attempts
- Regularly review and update security practices as new threats emerge

Remember that security is not a one-time setup but an ongoing process. The goal is to create robust defenses while maintaining the ability to effectively manage your digital assets. As the value locked in DeFi protocols grows, the importance of implementing these security measures becomes increasingly critical.