In collaboration with acceligence

Corporate Director Cyber Health Check

"Board directors occupy a position of exceptional access and influence, placing them at high risk of becoming a target of malicious cyber threat actors."

— NACD, Personal Cybersecurity Protection Guide for Corporate Directors

Cybersecurity threats are no longer just an IT concern: they're a boardroom issue. If you sit on a board, you're already a target, and attackers know how to exploit vulnerabilities to their advantage. These straightforward, practical steps will help you protect your personal digital life and strengthen the cybersecurity posture of the organizations you serve.

- [ ] **1. Use biometric authentication and passkeys instead of passwords wherever supported**

  Passkeys and biometrics are far more secure than traditional passwords and eliminate the risk of stolen credentials through phishing or reuse. If you must use passwords, ensure they are complex, unique, and changed periodically.

- [ ] **2. Turn on multi-factor authentication (MFA) everywhere possible**

  MFA adds a critical second layer of defense, preventing attackers from accessing your accounts even if they steal your password.

- [ ] **3. Secure your personal devices**

  Personal devices such as your laptop, phone, and tablet should use strong device passcodes, enable automatic locking, encrypt storage, and ensure remote wipe is activated in case of loss or theft. Use and update your antivirus and cybersecurity protection software regularly.

- [ ] **4. Stay alert to email and text-message-based phishing and social engineering attempts**

  Remain skeptical of unexpected messages, links, or requests - especially those that create urgency or ask for credentials or money.

- [ ] **5. Secure your personal email and online accounts**

  Review your email security settings, recovery options, and forwarding rules regularly - attackers often exploit these to stay hidden. Configure login and activity alerts (such as transaction and spending alerts) whenever possible.

- [ ] **6. Keep software, apps, and devices updated**

  Updates fix critical security flaws that can expose your data and put you at risk; turn on automatic updates wherever possible to stay protected against emerging threats.

7. Be mindful of what you and your loved ones share on social media

Personal details shared online — even seemingly harmless ones — can be exploited by attackers for social engineering, impersonation, or targeted phishing. Be cautious about what you post publicly and remind family members to do the same.

8. Use encrypted networks at home & on-the-go and avoid public Wi-Fi

Public networks are easy targets for interception - protect your data by using encrypted connections (like VPNs) and dedicated mobile hotspots. Home networks should be secured with strong Wi-Fi passwords.

9. Separate personal, professional, and board communications wherever possible

Keep work and board business off personal email and devices; use approved channels to reduce risk and preserve confidentiality. Ask your organization's Chief Information Security Officer (CISO) for guidance on the proper ways to communicate and stay secure.

10. Sync and backup your files and devices to a secure cloud storage service

Regular, encrypted backups ensure your critical data can be recovered quickly if your device is lost, stolen, or compromised.

11. Freeze and monitor your credit files at all credit bureaus and activate digital threat protection for you and your family

Credit freezes, identity monitoring, and dark web alerts reduce the risk of financial fraud and identity theft.

12. Protect your family's digital footprint and devices and talk to your loved ones about digital safety

Attackers often target family members - share basic cyber safety practices and make sure everyone's devices are secured. Talk to children and grandchildren about digital stranger danger and how to protect themselves from online threats.

13. Have a personal incident response plan

Know who to contact, what steps to take, and how to limit damage if your accounts or identity are compromised. Consider personal cybersecurity and/or identity theft insurance to help recover and remediate should a breach occur.

Additional resources

- Explore **NACD's cyber and technology insights, reports, and certification programs** to deepen your expertise as a strategic leader in the digital age. Visit **nacdonline.org/security** for more information.
- For more information or personalized guidance on protecting yourself and your family, contact us anytime at **hello@acceligence.com** or **+1 (312) 800-0800.**