FREE RESOURCE — EPISODE #16

Home & Small-Business Cybersecurity Checklist

Simple, actionable steps to secure your devices, data, and accounts — at home, at work, and in public.

Looking Forward Our Way

Nice Guy Technology

> Based on our conversation with **Mason & Mary Landrum** of Nice Guy Technology — use this checklist to work through your tech safety in about 30 minutes. Check each box as you complete it.

🔑 PASSWORD SECURITY

- [ ] **Use long passphrases** instead of short random passwords.
  E.g. "BlueDog!RunsFast99" — length beats complexity.
- [ ] **Never reuse passwords** across different accounts.
  One breach shouldn't unlock everything else you own.
- [ ] **Install a password manager** (Bitwarden, 1Password, or LastPass).
  It remembers everything — you only need one master password.
- [ ] **Enable two-factor authentication (2FA)** on email and financial accounts.
  Use an authenticator app — not just SMS when possible.

☁️ CLOUD & DATA BACKUPS

- [ ] **Know where your data lives** — on the device, cloud, or both?
  If it only exists on your laptop, one failure loses it forever.
- [ ] **Set up cloud backup** (OneDrive, Google Drive, or Dropbox).
  Automated daily backup — set it and forget it.
- [ ] **Keep a local backup** on an external drive (weekly).
  Two backup layers = recovery from ransomware without paying.
- [ ] **Test your backup** by restoring one file as a drill.
  An untested backup is not a real backup.

💻 DEVICE & ENDPOINT PROTECTION

- [ ] **Install reputable endpoint protection** (antivirus/anti-malware).
  Windows Defender is solid; Malwarebytes is a trusted add-on.
- [ ] **Keep your OS and software updated** — enable automatic updates.
  Most breaches exploit known, already-patched vulnerabilities.
- [ ] **Physically clean devices quarterly** — compressed air in vents.
  Overheating from dust is a leading cause of hardware failure.
- [ ] **Enable device encryption** (BitLocker on Windows, FileVault on Mac).

📶 PUBLIC WI-FI & REMOTE WORK

- [ ] **Never do sensitive work on open public Wi-Fi.**
  Banking, email, and admin tasks only on trusted networks.
- [ ] **Use your phone's personal hotspot** when working in coffee shops.
  Your carrier's network is encrypted; the café's Wi-Fi is not.
- [ ] **Use a business VPN** if your employer provides one — always.
  VPN encrypts all traffic between your device and the server.
- [ ] **Lock your screen** any time you step away from your device.

Protects your data if a device is lost or stolen.

Physical access is the easiest security breach of all.

🚨 IF SOMETHING GOES WRONG — RESPONSE CHECKLIST

- ☐ **Disconnect from the internet** immediately if you suspect ransomware or active breach.
- ☐ **Do NOT pay the ransom** — contact a professional IT firm first to assess recovery options.
- ☐ **Change all passwords** from a clean, unaffected device immediately after a breach.
- ☐ **Notify your bank** if financial accounts may have been compromised.
- ☐ **Check haveibeenpwned.com** to see if your email appears in known data breaches.
- ☐ **Document everything** — screenshots, dates, and communications for insurance or legal purposes.

💡 **Quick Win:** Start with passwords and backups — they protect the most people for the least effort. If you need hands-on help, Mason and Mary Landrum at **Nice Guy Technology** offer small-business IT support and can help you implement these steps. To learn more, listen to Episode #16 of the **Looking Forward Our Way Podcast** at lookingforwardourway.com.

Need hands-on help?
Contact Nice Guy Technology for small-business IT support.
hello@lookingforwardourway.com · lookingforwardourway.com

Looking Forward Our Way Podcast
lookingforwardourway.com