CYBERGUARD INCIDENT RESPONSE

Emergency Security Checklist

PHASE 1 — DETECTION

- ☐ Unexpected password change emails
- ☐ Can't log into accounts
- ☐ Unknown posts/messages from you
- ☐ Strange bank transactions
- ☐ Friends reporting suspicious messages
- ☐ Device acting slow or strange

PHASE 2 — CONTAINMENT

- ☐ Disconnect internet immediately
- ☐ Unplug external drives
- ☐ Switch to clean device
- ☐ Change email password
- ☐ Change banking passwords
- ☐ Change social media passwords

PHASE 3 — ERADICATION

- ☐ Change passwords + enable 2FA
- ☐ Remove suspicious email rules
- ☐ Revoke unknown connected apps
- ☐ Sign out all devices
- ☐ Run full malware scan
- ☐ Update all software

PHASE 4 — RECOVERY

- ☐ Restore from clean backup
- ☐ Reset all passwords again
- ☐ Enable 2FA on every account
- ☐ Update recovery phone/email
- ☐ Notify contacts if spam sent

PHASE 5 — ANALYSIS

- ☐ Identify how attacker entered
- ☐ Check haveibeenpwned.com
- ☐ Review login history
- ☐ Inspect email forwarding rules
- ☐ Document evidence/screenshots

PHASE 6 — HARDENING

- ☐ Use password manager
- ☐ Unique password per site
- ☐ Authenticator app (not SMS)
- ☐ Frequent updates
- ☐ Perform security audits

EMERGENCY CONTACTS

Bank Fraud Line: _____

Mobile Carrier: _____

Local Police: _____

FTC Identity Theft: identitytheft.gov

IC3 (FBI): ic3.gov

CyberGuard Discord: https://discord.gg/JXPjRXQV