🛡️ THE ONLINE SCAM SPOTTER'S CHECKLIST

Your Digital Shield Against Online Predators

Survive Backpacking - Recon Specialist Protocol

Operator's Protocol: Trust is earned, not given. In the digital battlefield, your skepticism is your strongest weapon. Use this checklist before clicking, sending, or sharing anything online.

🚨 RED FLAGS - ABORT IMMEDIATELY

- [ ] Asks for passwords or login credentials
- [ ] Demands immediate action ("Act now or lose this!")
- [ ] Requests wire transfers, gift cards, or cryptocurrency
- [ ] Claims you've won something you didn't enter
- [ ] Poor grammar, spelling, or formatting
- [ ] Generic greetings ("Dear Customer")
- [ ] Threatens legal action or account suspension
- [ ] Asks for Social Security or ID numbers
- [ ] Sender email doesn't match company domain
- [ ] Links hover-preview shows different URL
- [ ] "Too good to be true" offers or deals
- [ ] Emotional manipulation or fear tactics
- [ ] Requests remote access to your computer
- [ ] Unsolicited investment opportunities

🔍 VERIFICATION PROTOCOL - BEFORE YOU ENGAGE

- [ ] Check sender's email address carefully
- [ ] Hover over links without clicking
- [ ] Search company name + "scam"
- [ ] Call company using official number
- [ ] Check website security (https://)
- [ ] Verify social media accounts exist
- [ ] Read reviews on multiple platforms
- [ ] Check business registration/licensing
- [ ] Reverse image search profile photos
- [ ] Verify phone numbers independently
- [ ] Ask specific questions only real person would know
- [ ] Request video call for high-value interactions
- [ ] Check if deal exists on official website
- [ ] Trust your gut - if it feels off, it is
- [ ] Get second opinion from trusted friend

🛡️ OPERATOR'S GOLDEN RULES

Never give personal info to unsolicited contacts • Use strong, unique passwords • Enable 2-factor authentication • Keep software updated • When in doubt, don't click, don't send, don't engage

🚨 COMMON SCAM TYPES - STAY ALERT

⚠️ PHISHING EMAILS

Fake emails from "banks," "PayPal," "Amazon" asking you to click links to "verify" account info. Always log in directly to the official website instead.

⚠️ INVESTMENT SCAMS

"Guaranteed returns," crypto schemes, or pressure to invest quickly in "limited opportunities." Real investments have risks.

⚠️ ROMANCE SCAMS

Online "relationships" that quickly turn to requests for money, travel funds, or emergency help. Real love doesn't ask for wire transfers.

⚠️ WORK-FROM-HOME SCAMS

Jobs requiring upfront payment, personal info, or seem too easy for the promised pay. Legitimate jobs pay you, not the other way.

⚠️ TECH SUPPORT SCAMS

Pop-ups or calls claiming your computer is infected and offering to "fix" it for payment. Microsoft doesn't call you randomly.

⚠️ FAKE SHOPPING SITES

Ultra-cheap prices, no contact info, poor website design, or no customer reviews. If the deal seems impossible, it probably is.

🚨 IF YOU'VE BEEN TARGETED - IMMEDIATE ACTION

Emergency Response Protocol:

- ☐ **Don't panic** - you're not the first, won't be the last
- ☐ **Change passwords** immediately on all relevant accounts
- ☐ **Contact banks/credit cards** to alert them of potential fraud
- ☐ **Document everything** - screenshots, emails, transactions
- ☐ **Report to authorities** - FTC at reportfraud.ftc.gov
- ☐ **Alert your network** - friends/family might be next targets
- ☐ **Monitor accounts** closely for unauthorized activity
- ☐ **Consider identity monitoring** services if personal info compromised

📞 EMERGENCY CONTACTS & RESOURCES

Federal Trade Commission (FTC)
Report: reportfraud.ftc.gov
Phone: 1-877-FTC-HELP

Social Security Administration
Report: ssa.gov/scam
For SSN-related scams

Internet Crime Complaint Center
Report: ic3.gov
For internet-related crimes

Your Bank & Credit Card Companies
Use numbers on back of cards
NOT numbers in suspicious emails