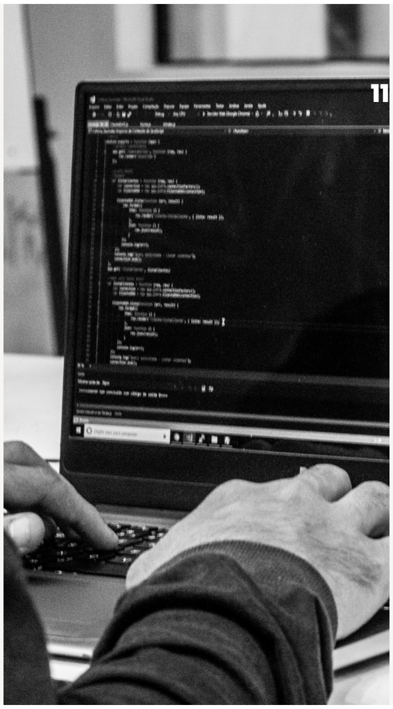
CMIT Solutions®
Your Technology Team

CyberHoot
Become More Aware | Become More Secure

Cybersecurity 2023:

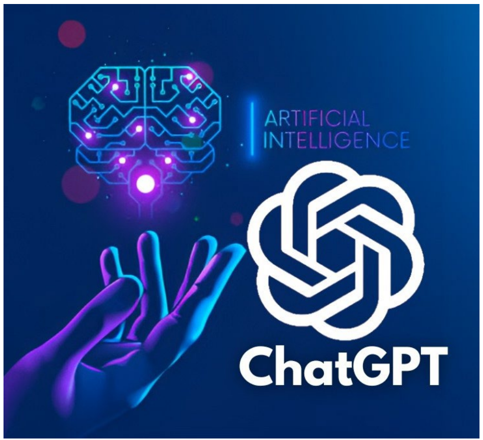
**Essentials for Small Business:
Protecting Your Digital Assets in the
Modern Age**

**Every employee needs these
Cyber Literacy skills
to stay safe online.**



Common Cyber Crime Attacks

- Ransomware
- Business Email Compromise
- Remote Access Trojans
- Wire Fraud



ChatGPT can write this malware for you! Fewskillz required.

Cybersecurity Preparedness

The Three Pillars

1 Policy & Process

1. Risk Assessment is key!

2. Cyber Governance Policy

3. Patching and Incident Mgmt. Processes

2 People

4. Teach **Cyber Literacy**
   - Attackers
   - Methods
   - Cybersecurity skills to prevent
5. Run educational Phishing Tests and Simulations (demo ahead)

3 Technology

6. Deploy and validate Safeguards
   - Two-Factor Authentication
   - Password Manager
   - Anti-virus, End Point Protection
   - Email Security (SPAM)
   - Backups (Verify)
7. Data Privacy
8. Cyber Insurance

Two Skills for the 21st Century

90% of all breaches are caused by human error: a Social Engineering attack leading to password compromise or a successful phishing attack.

Avoiding Phishing emails:

Understand the #1 online threat you face.

Learn 6 questions to ask.

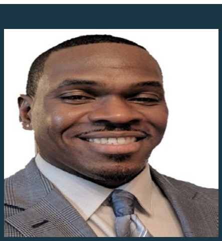
Spot and delete phishing attack emails.

Employee Call to Action

- With 90% of breaches traced to human error, employees must learn:
  - good password hygiene
  - A password manager, and
  - how to spot and avoid phishing attacks

  to protect themselves personally and professionally.

CMIT Solutions®
Your Technology Team



Roderick Floyd

OWNER / PRESIDENT | CMIT SOLUTIONS OF ARLINGTON

rfloyd@cmitsolutions.com