

The real problem

“The human factor is truly security’s weakest link.”

**The Art of Deception
by**

Kevin Mitnick, convicted Cyber Criminal



The Magnitude of the Threat


- **90% of breaches are caused by human error or carelessness (IBM)**



- **In 2018, 90% of American adults** had their personal information stolen by hackers, primarily through data breaches at large companies (CBS)



Important Concepts

1. Job #1: Backups, Business Continuity, and Disaster Recovery 
2. There is no Privacy on the Internet
3. Information about you and your firm is easily accessible
4. Nothing is free on the Internet
5. Be vigilant always

~~Privacy~~

What do Facebook, Apple, Amazon, Netflix, Google, Microsoft, your Internet provider, and the Government know about you?

- **EVERYTHING!**

- **Your IQ**
- **Personal interests, likes, dislikes**
- **Browsing history**
- **Habits**
- **When you access the Internet, check mail**



The perpetrators – Who are they?

And why do they do it?

- **Insiders**
- **Individuals, Lone Wolves**
- **Hacktivist**
- **State Sponsored Teams**
- **Criminal Networks**



Who are the Targets?

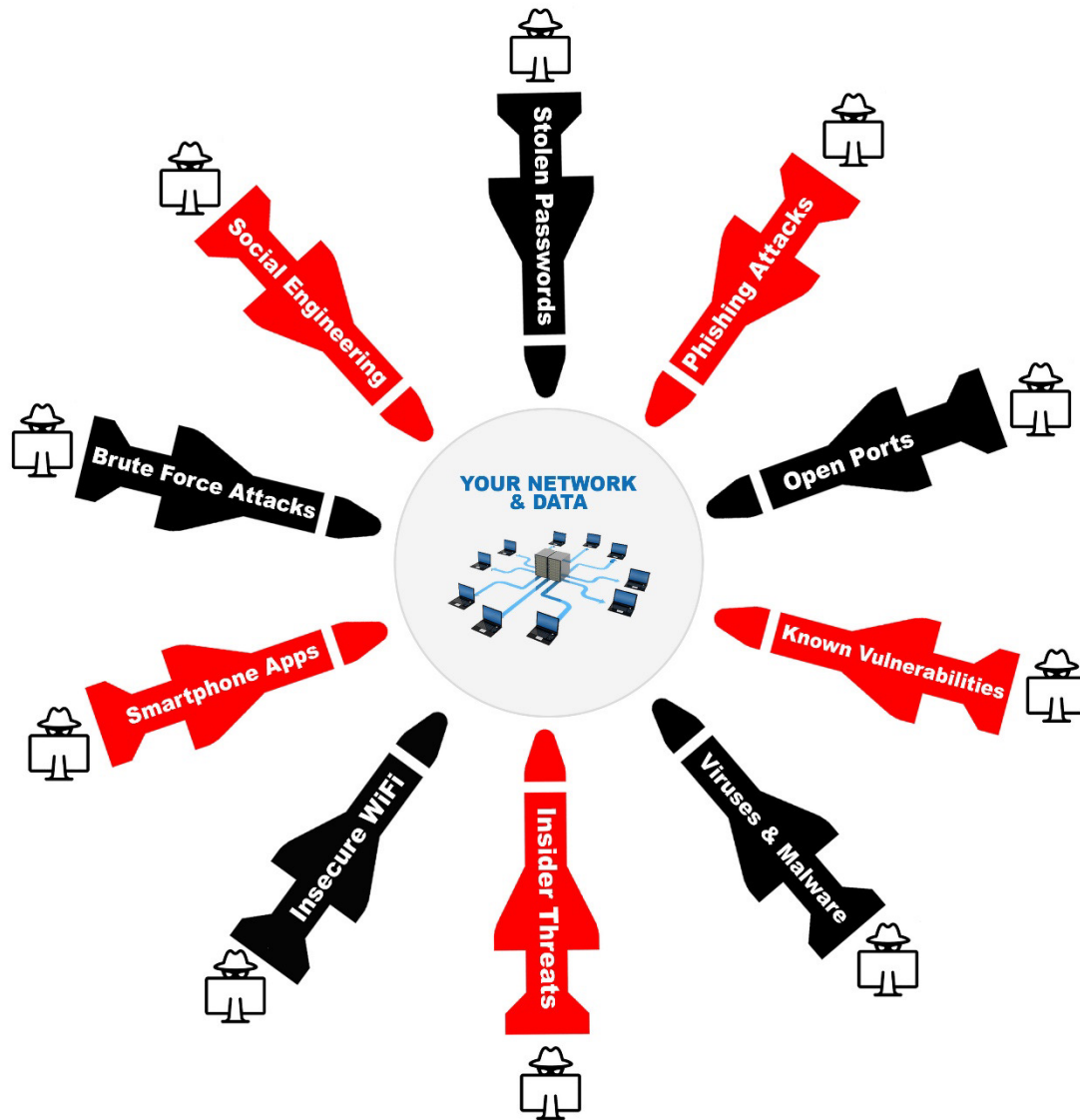
- EVERYONE!



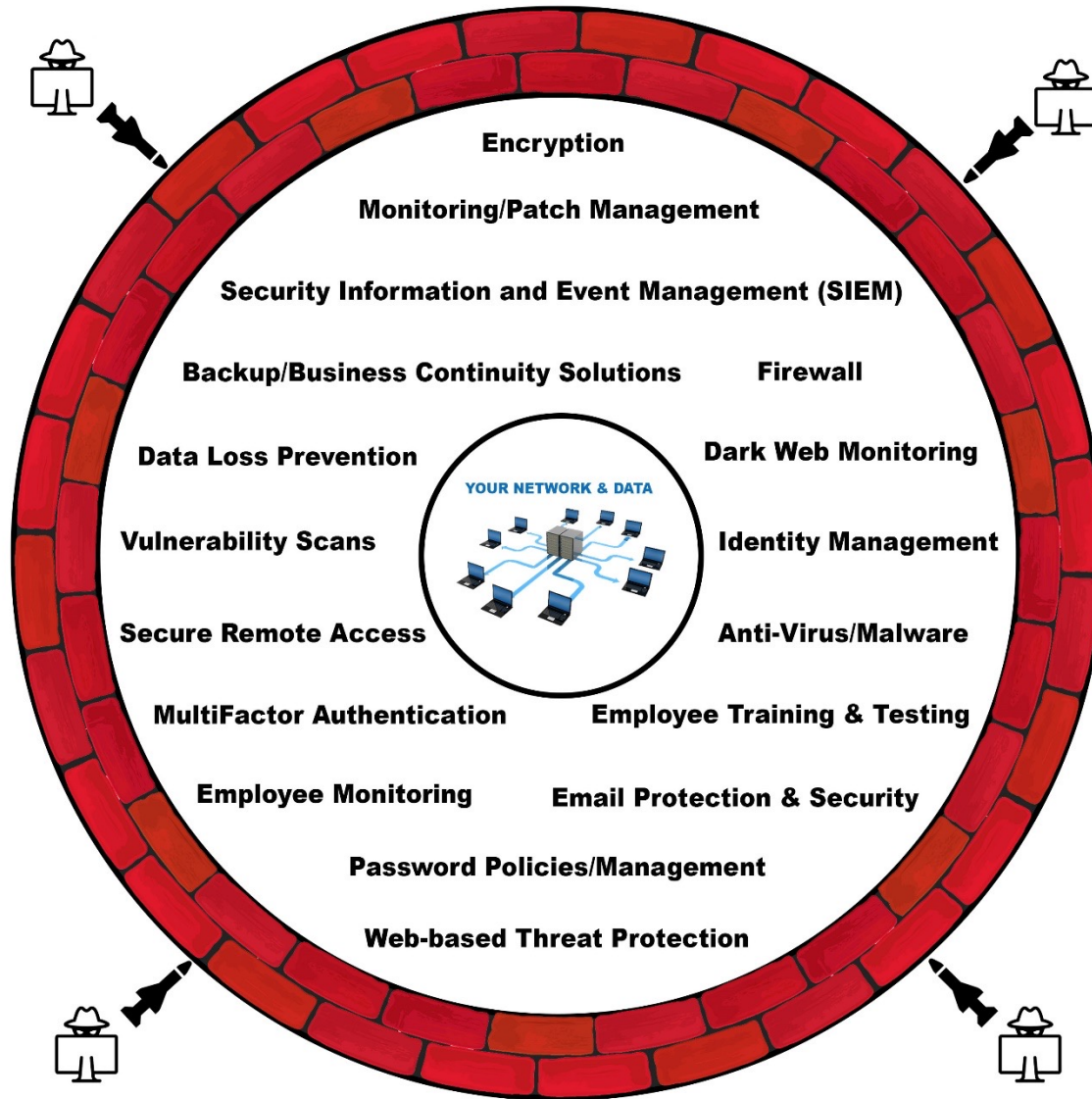
- 90% of all attacks are against businesses with < 1,000 employees

1/3 of all breaches are against companies with < **100** employees

Your Vulnerabilities and the Weapons Used Against you



Cyber Security Solutions You Need To Stay Safe



Yes, it is overwhelming!

You can't do it alone!

Listen to your I.T. Provider

Don't wait until you are breached

They should have a Cyber Security Checklist

If they don't, find another one that does

Put an ongoing plan in place



Corona Virus and the Expanded “Attack Surface”

Remote workers on unsecured networks

Vaccine scams

Mis-information

Dis-information



Corona Virus and Computer Viruses

They both Replicate and Mutate!

2007: Self morphing viruses



- 2007 – 2009 Self morphing viruses/Zeus Virus
- 2011 – 300% increase in cyber –attacks
- 2013 – Attacks targeted at contents of RAM (Target)
- 2014 – SSL Vulnerability (Heartbleed), Sony hack
- 2015 – Massive attack at U.S. Office of Personnel Management
- 2016 – Ukraine Power Grid Hack disclosed
- 2017 – Podesta, Swift, Equifax, many others
- **2018 - 2021 – Too many to list!**

Infection Methods

PHISHING:



Credential Harvesting results in
TODAY'S BIGGEST THREAT
Business Email Compromises!
“BEC’s”

Infection Methods

Credential Harvesting:



1. Phishing sends you to a website
2. Looks like one of your typical login pages (email, banking, etc.)
3. You put in your credentials
4. They now have full access to everything
5. They can sit there for months, exfiltrating data, emails, and phishing all your contacts

They are in mailboxes for an average of 2.5 months!

Phishing Methods

- Phishing
- Spear Phishing
- Whaling
- Vishing
- Smishing
- Search Engine Phishing



NEVER engage the hacker by responding in any way!

“Drive-by Infections”

- 1 in 8 web pages are infected.
9500 per day (Google statistic)
- Be very suspicious.
- This is how Ransomware works!
- NEVER click on a link unless you are absolutely sure it is safe!
- If requested to change your password for a site – DO NOT CLICK ON THE LINK! Delete the email, open your browser, log into the site manually, and change the password.
- **Confirm the identity of anyone that sends you a link or attachment**



Social Networking Sites

- Facebook, Twitter, Google+, Pinterest, thousands of them
- The good, the bad, and the ugly
- Once it is on the Internet it never goes away!
- Be careful what you post.
- Don't be stupid!



Smartphones

- More than 50% take your personal info
(Wall Street Journal)
- Delete the ones you do not use
- Use biometrics and STRONG passwords
- Wipe your phone before discarding it
- Location services – the good and bad
- The microphone and camera



Wireless Networks



- Great technology if they are secured. Hacker's paradise if not.
- If it does not require a password, it is OPEN and ***less secure!***
- At home: Use passwords for encryption.
- Use your own personal hotspot (Smartphone, AT&T Velocity, Verizon JetPack)

USB Flash drives / Thumb drives



- Powerful tools for a hacker
- Easy to embed with a virus
- The Iranian nuclear program put back 2-3 years
- Only use brand names
- Never use one you “found”
- Always be sure your anti-virus is up to date and configured to scan anything that is plugged into your computer
- What companies are doing – No USB, no DVD
- Do not use public USB Charging Stations

Social Engineering

- “Psychological manipulation of people into performing actions or divulging confidential information.” – Wikipedia
- The latest and often the most effective tool
- Some scenarios – “I’m from the help desk, Microsoft, the IRS, your bank.....”



NEVER engage the hacker by responding in any way!

Physical Security



- Lock the doors!
- Lock your computer: CTRL-ALT-DEL – Lock Computer
- Logoff your computer: Start – Shutdown – Logoff
- Do not leave passwords written next to computer
- Notebook computers with Confidential Data – Use Encryption

Logical Security



Passwords! The single most important defense

Change your passwords regularly!

Make them Unique

Different ones for each site, application, system

Make them complex

Minimum 8 characters, 3 of these: Upper, Lower, Numbers, Symbols

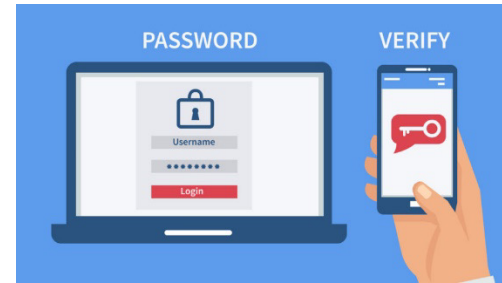
Keep them Private! Do not write them on a Post-it note

Do NOT store them in your browser!

Can't remember them? Use Last Pass



Logical Security



Use 2-Factor/Multi-Factor Authentication (2FA, MFA) wherever possible

Stops more than 90% of all BEC's (Business Email Compromises)

Logical Security



Never e-mail PII !!!!

(Personally Identifiable Information)

**Use secure encrypted portals to share
files containing PII**

Logical Security



Check your bank accounts daily

Check your credit card accounts monthly

Freeze your Credit Reports

A word about the future of Cyber Security techniques

- Zero day threats, password hacking, and stealth malware are the problem
- Firewalls and Anti-Virus are useless against them
- The answer?
- **SIEM: Security Information and Event Management**
- **Utilizing Behavioral Analytics and Artificial Intelligence**





Here's the Good News!
The bad guys are brutally pragmatic.
They like easy 'soft' targets
and there are plenty of them.
Be a HARD target!

What you can do at work and home to protect yourself

1. Backup personal data to the cloud: Carbonite, Mozy, iBackup.
2. Change your passwords, make them strong, keep them private. NEVER use the same password for more than one site. Use Last Pass or another secure password manager.
3. Use 2-Factor/Multi-Factor Authentication (2FA, MFA) wherever possible.
4. Keep your Computer, Anti-Virus, Browsers, Flash & Java up to date. No Win 7, XP, Vista
5. Configure Anti-Virus to scan anything plugged in to your computer.
6. Beware of unsolicited links or attachments. Never open a link or attachment unless you are ABSOLUTELY sure it is safe. Report anything that is suspicious – DO NOT CLICK ON IT!
7. Beware of Pop-ups telling you that you need to call to remove a virus or update/optimize your computer. If you get one, close out of all programs and reboot your computer. NEVER call the number on the screen.
8. NEVER allow anyone to access your computer unless you are absolutely sure they are from your corporate help desk. If you are unsure, call your corporate help desk to confirm that they are who they say they are.
9. Beware of phone scams – “I’m from the Help Desk, Microsoft, the IRS, your bank....” HANG UP the phone immediately. NEVER engage the hacker in any way!
10. Lock your computer when you are leaving it for any period of time.
11. Logoff your computer every night. Leave it on, though, so it can receive updates.
12. Reboot your computer at least once a week.
13. NEVER email Personally Identifiable Information (PII). Use secure encrypted portals to share files containing PII.



What you can do at work and home to protect yourself

- 14. Never e-mail work products to your personal email account.**
- 15. Never use Flash Drives you “found” or ones given to you. Buy and use brand names.**
- 16. Smartphones: Beware of the apps you use. Delete the ones you don’t use.**
- 17. Smartphones: Use biometrics & strong passwords. Wipe them before discarding them.**
- 18. Never use public USB charging stations- Always use your own charger.**
- 19. Encrypt laptops that have PII or confidential data on them.**
- 20. Only use secure websites (<https://>) when entering any personal or financial information (credit card numbers, Social Security Number, Driver’s License, etc.).**
- 21. Always convert sensitive files to PDF before sending them to strip out metadata.**
- 22. Never use “free” music/video sharing sites. Legitimate streaming sites like Pandora and Spotify are fine, though.**
- 23. Protect and encrypt your wireless networks with passwords.**
- 24. Check your bank accounts daily and credit cards at least monthly for suspicious activity.**
- 25. Freeze your credit reports. It is easy and it is the best protection against identity theft.**
- 26. If you think you have been breached: TURN OFF THE COMPUTER and CALL FOR HELP!**

Questions



AT&T
Business



Somerset County
Business Partnership



ALPINE
BUSINESS SYSTEMS, INC.

