Cyber Security Training Seminar

ALPINE
BUSINESS SYSTEMS, INC.

CELEBRATING
30
YEARS
2017

Bill Blum

ALPINE
BUSINESS SYSTEMS, INC.

CELEBRATING 30 YEARS 2017

The real problem

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

The Art of Deception

by

Kevin Mitnick, convicted CyberCriminal

The goal of all Cybersecurity Policies and Procedures:

ALPINE BUSINESS SYSTEMS, INC.
CELEBRATING 30 YEARS 2017

The goal of all Cybersecurity Policies and Procedures:

An acceptable balance between:

Functionality, Usability, and Risk.

The goal of all Cybersecurity Policies and Procedures:
An acceptable balance between:
Functionality, Usability, and Risk.

The only way to be totally secure is to not connect to anything.

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

The Magnitude of the Threat

- If “Hackers Inc.” was a company:
  - #1 on Fortune 500
  - 74x the size of Walmart

The Magnitude of the Threat

- If "Hackers Inc." was a company:
  - #1 on Fortune 500
  - 74x the size of Walmart
- In 2018, **90% of American adults** had their personal information stolen by hackers, primarily through data breaches at large companies (CBS)

The Magnitude of the Threat

- If “Hackers Inc.” was a company:
  - #1 on Fortune 500
  - 74x the size of Walmart
- In 2018, 90% of American adults had their personal information stolen by hackers, primarily through data breaches at large companies (CBS)
- **Total global cost of breaches: $2,430,000,000,000 Yes TRILLION! Average cost: $3.8 million (IBM)**

ALPINE BUSINESS SYSTEMS, INC.
CELEBRATING 30 YEARS 2017

The Magnitude of the Threat

- If “Hackers Inc.” was a company:
    - #1 on Fortune 500
    - 74x the size of Walmart
- In 2018, 90% of American adults had their personal information stolen by hackers, primarily through data breaches at large companies (CBS)
- Total global cost of breaches: $2,430,000,000,000,

    Yes TRILLION! Average cost: $3.8 million (IBM)
- **90% of breaches are caused by human error or carelessness (IBM)**

The Federal Government

- **The FBI**

The Federal Government

- The FBI
- **The President**

The Federal Government

- The FBI
- The President
- **The Joint Chiefs of Staff**

Cyber Mission Force: 140+ teams

5 Important Concepts

- **Job #1: Backups, Business Continuity, and Disaster Recovery**

5 Important Concepts

- Job #1: Backups, Business Continuity, and Disaster Recovery
- **There is no Privacy on the Internet**

5 Important Concepts

- Job #1: Backups, Business Continuity, and Disaster Recovery
- There is no Privacy on the Internet
- **Information about you and your firm is easily accessible.**

5 Important Concepts

- Job #1: Backups, Business Continuity, and Disaster Recovery
- There is no Privacy on the Internet
- Information about you and your firm is easily accessible.
- **Nothing is free in life or on the Internet**

5 Important Concepts

- Job #1: Backups, Business Continuity, and Disaster Recovery
- There is no Privacy on the Internet
- Information about you and your firm is easily accessible.
- Nothing is free in life or on the Internet
- **Be vigilant always**

Privacy

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

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 difference between

Microsoft

Google

The difference between

Microsoft Software

Google

The difference between

Microsoft   Software

Hardware

Google

The difference between

Microsoft	Software
	Hardware
Google	Ad Agency

Nothing is free

- **What you give up for free technology:**

A LOT of information about you, your life, your family, friends,

EVERYTHING

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Privacy

- One of today's biggest technology issues
- The 1979 Smith Decision
- The EU's General Data Protection Regulations
- California's Consumer Privacy Act
- Facebook's Zuckerberg on the hot seat
- Apple's Ad campaign
- 2019: Personal data is worth more than oil
- Edward Snowden – We are talking about people, not data

Nothing is free

- **Criminals make offers too good to be true**
  - **Free music, videos**
  - **Free money**

Nothing is free

- What you give up for free technology
- Criminals make offers too good to be true
  - Free music, videos
  - Free money
- Senior Citizens Beware!

Be Vigilant Always

- **The criminals work 24/7/365 – they have robots**

Be Vigilant Always

- The criminals work 24/7/365 – they have robots
- **“Only the Paranoid Survive,” Andy Grove**
  - **Co-founder and CEO of Intel**

Be Vigilant Always

- The criminals work 24/7/365 – they have robots
- “Only the Paranoid Survive,” Andy Grove
  - Co-founder and CEO of Intel

- **Everyone and every company is under attack**

Be Vigilant Always

The old way of thinking

There are only 2 kinds of companies

Be Vigilant Always

The old way of thinking

There are 2 kinds of companies:

1. Those that know they are under attack

2. Those that don’t

Be Vigilant Always

The *NEW* way of thinking

There are only 2 kinds of companies

1. Those that *have* been breached

2. Those that *will* be breached

(the FBI and Lowell McAdam, Verizon CEO)

- **2007 – Self morphing viruses**

- 2007 – Self morphing viruses

- **2009 – Zeus Virus – the man in the browser – NO browser is safe**

- 2007 – 2009 Self morphing viruses/Zeus Virus
- **2011 – 300% increase in cyber –attacks**

- 2007 – 2009 Self morphing viruses/Zeus Virus
- 2011 – 300% increase in cyber –attacks
- **2013 – Attacks targeted at contents of RAM (Target)**

- 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**

- 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**

- 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**

- 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**

- 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 and 2019 – Too many to list!**

The perpetrators – Who are they? And why do they do it?

5 Distinct Groups

The perpetrators – Who are they? And why do they do it?

- Insiders

The perpetrators – Who are they?
And why do they do it?

- Individuals, Lone Wolves

The perpetrators – Who are they? And why do they do it?

- Hacktivists (Anonymous and others)
  - Infamous Estonia hack

The perpetrators – Who are they? And why do they do it?

- State-sponsored Terrorists
  - China, North Korea, Russia, Iran

WANTED
BY THE FBI

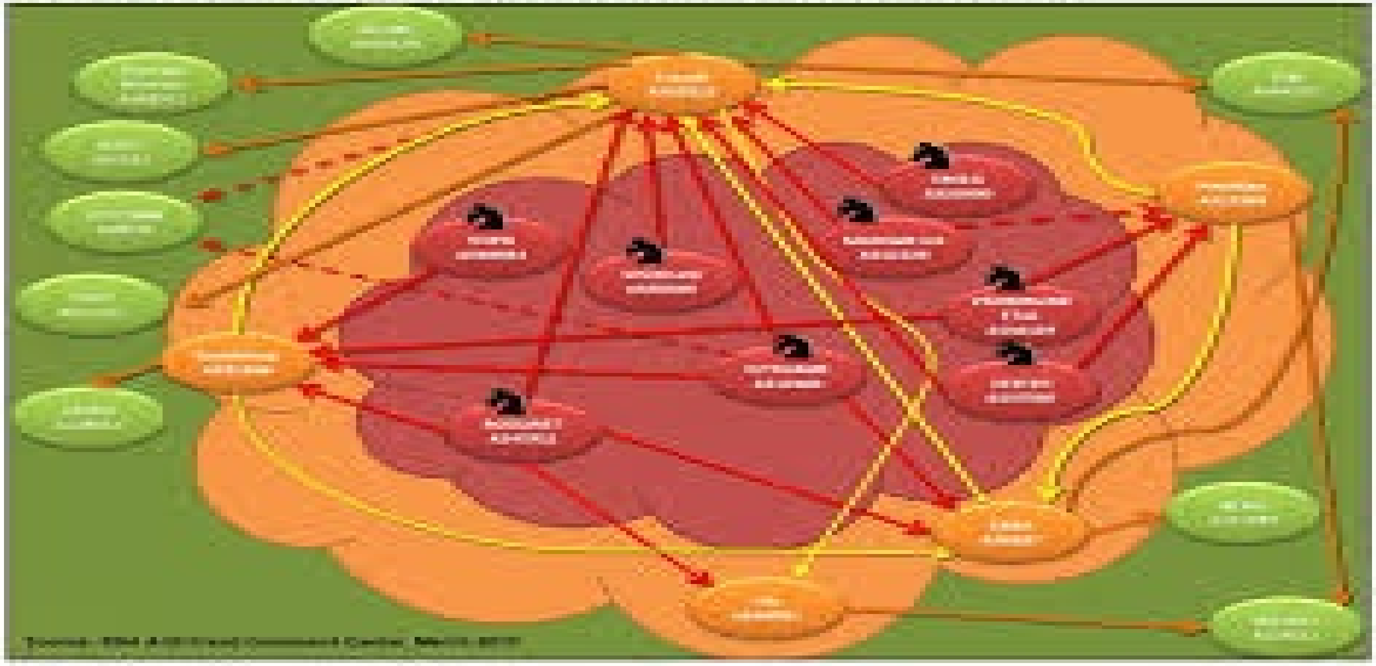
Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu   Wen Xinyu   Sun Kailiang   Gu Chunhui   Wang Dong

The perpetrators – Who are they? And why do they do it?

- Well Organized Criminal Networks

Figure 2: The Cybercrime Infrastructure, and the ISP's that connect it to the internet



Source: RSA Anti-Fraud Command Center, March 2011

Image Legend:

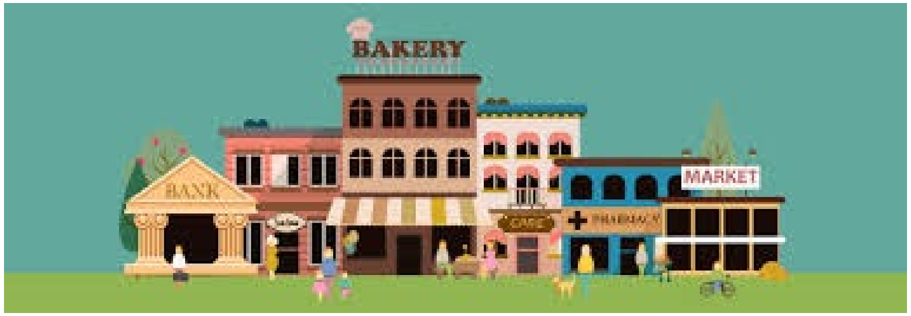
Bulletproof Networks where malware is actually hosted are marked in red with the Trojan horse's icon sign;

Upstream Providers are orange-colored spheres;

Who are the Targets?

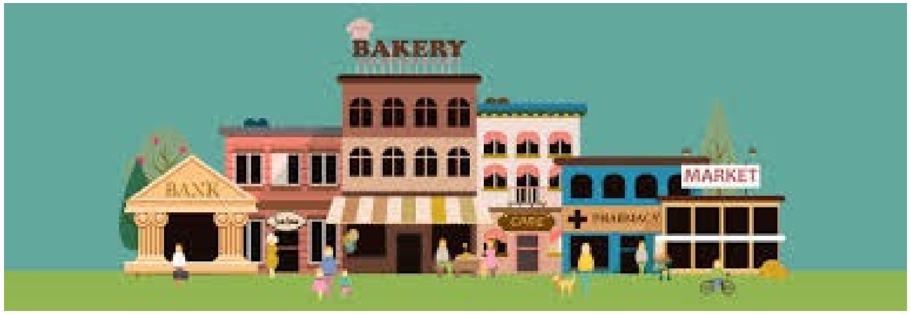
Who are the Targets?

EVERYONE!



Who are the Targets?

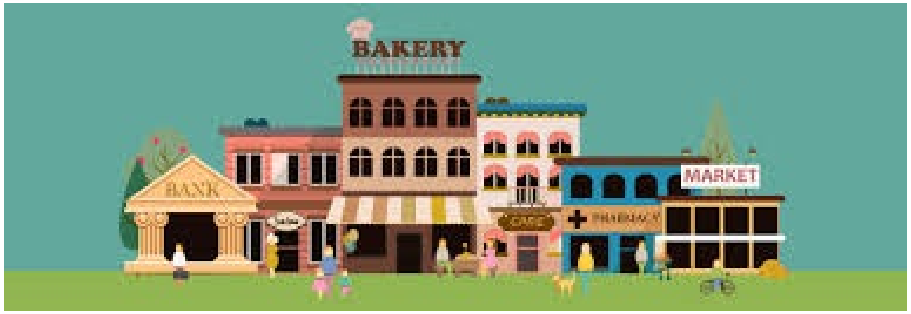
- EVERYONE!



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

Who are the Targets?

- EVERYONE!



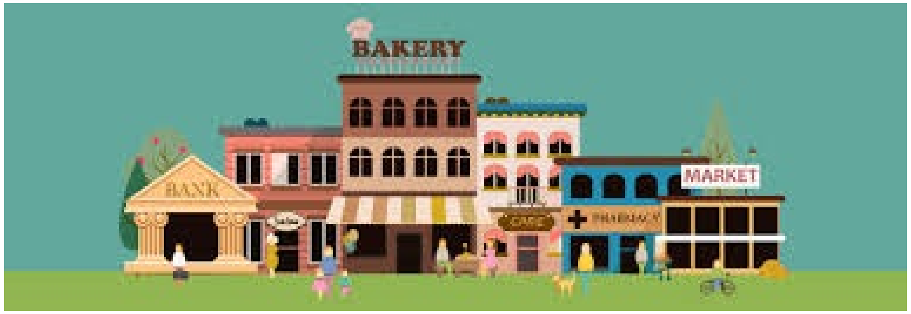
- 90% of all attacks are against businesses with < 1,000 employees

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

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

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

Retailers are attacked most.

3x more than the previous #1 targets,

financial institutions

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Tools of the Trade

Viruses

Spyware

Malware

Tools of the Trade

Viruses

Spyware

Malware

- **Hundreds of attempts foiled every week**

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Tools of the Trade

Viruses

Spyware

Malware

- Hundreds of attempts foiled every week
- Designed to steal or corrupt data and information

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Tools of the Trade

Viruses

Spyware

Malware

- **Multiple methods of infection**

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Tools of the Trade

Viruses

Spyware

Malware

- **Multiple methods of infection:**

emails, texts, *web sites*

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Infection Methods

Emails using Spam

- 98% of all email is SPAM
- Easy to create
- Easy to spoof addresses (impersonate someone else)

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Infection Methods

Emails

- Viruses in email attachments

Infection Methods

Others:

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

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Infection Methods

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

NEVER engage the hacker by responding in any way!

Infection Methods

Most Result in:

Links to infected web sites!

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

“Drive-by Infections”

1 in 8 web pages are infected
9500 per day (Google statistic)

Many contain Zero-day Viruses

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

“Drive-by Infections”

- 1 in 8 web pages are infected. 9500 per day (Google statistic)

Be very suspicious.

This is how Ransomware works!

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

“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!

“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!

- **Look for the name right before .com, .org, etc. in the URL**

“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!
- Look for the name right before .com, .org, etc. in the URL
- **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.**

“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!
- Look for the name right before .com, .org, etc. in the URL
- 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**

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Infection Methods

Texts

- Viruses in texts
- Incredibly dangerous
- Very expensive to build and deploy

The economics of virus/malware/spyware creation

- Individuals, crime gangs build them for their own use

The economics of virus/malware/spyware creation

- Individuals, crime gangs build them for their own use
- **They sell them, then give them away**

The economics of virus/malware/spyware creation

- Individuals, crime gangs build them for their own use
- They sell them, then give them away
- **Venture capital funded companies build them for BIG profits!**

The economics of virus/malware/spyware creation

- Individuals, crime gangs build them for their own use
- They sell them, then give them away
- Venture capital funded companies build them for BIG profits
- **Their clients:**
  - **Nation states**
    - **for spying, gathering intel, and theft**

The economics of virus/malware/spyware creation

- Individuals, crime gangs build them for their own use
- They sell them, then give them away
- Venture capital funded companies build them for BIG profits
- Their clients:
  - Nation states for spying, gathering intel, and theft
  - **U.S. Government agencies included**

General Michael Hayden
Former head of the NSA and CIA

General Michael Hayden
Former head of the NSA and CIA

- **Cyber warfare is more difficult than conventional warfare**

General Michael Hayden
Former head of the NSA and CIA

- Cyber warfare is more difficult than conventional warfare

- **Spy vs. Spy has been going on forever**

General Michael Hayden
Former head of the NSA and CIA

- Cyber warfare is more difficult than conventional warfare
- Spy vs. Spy has been going on forever

- **We do it and we are the best with the best tools**

General Michael Hayden
Former head of the NSA and CIA

- Cyber warfare is more difficult than conventional warfare
- Spy vs. Spy has been going on forever
- We do it and we are the best with the best tools

- **We do it for fundamentally different reasons than our adversaries**

General Michael Hayden
Former head of the NSA and CIA

- Cyber warfare is more difficult than conventional warfare
- Spy vs. Spy has been going on forever
- We do it and we are the best with the best tools
- We do it for fundamentally different reasons than our adversaries
- **There are “honorable” hacks:**

The Chinese vs. US OPM

General Michael Hayden
Former head of the NSA and CIA

- Cyber warfare is more difficult than conventional warfare
- Spy vs. Spy has been going on forever
- We do it and we are the best with the best tools
- We do it for fundamentally different reasons than our adversaries
- There are “honorable” hacks – The Chinese vs. US OPM

- **There are new, very dangerous ones: N. Korea vs. Sony**

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Transparency and Reporting:

The major shift in U.S. Policy

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: S**ecurity **I**nformation and **E**vent **M**anagement
- **Utilizing Behavioral Analytics and Artificial Intelligence**

ALPINE
BUSINESS SYSTEMS, INC.
CELEBRATING 30 YEARS 2017

Social Networking Sites

- Facebook, Twitter, Google+, Pinterest, thousands of them

- The good, the bad, and the ugly

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!**

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% of apps take your personal info (Wall Street Journal)

Smartphones

- More than 50% of apps take your personal info

  (Wall Street Journal)
- **Delete the ones you do not use**

Smartphones

- More than 50% of apps take your personal info

  (Wall Street Journal)

- Delete the ones you do not use
- **Use biometrics and STRONG passwords**

Smartphones

- More than 50% of apps 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**

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**

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.

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!**

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!

- **Be sure you only access HTTPS:// sites on OPEN WiFi Networks**

Wireless Networks

- Great technology if they are secured. Hacker's paradise if not.
- If it does not require a password it is OPEN and it is less secure!
- Be sure you only access HTTPS:// sites on open WiFi networks

- **At home: Use encryption.**

  WPA-PSK or stronger.

Wireless Networks

- Great technology if they are secured. Hacker's paradise if not.

- If it does not require a password it is OPEN

  and it is less secure!

- Be sure you only access HTTPS://   sites on open WiFi networks

- At home: Use encryption. WPA-PSK or stronger.

- **Use your own HotSpot (Smartphone, Verizon JetPack, AT&T Velocity)**

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

USB Flash drives / Thumb drives

- Powerful tools for a hacker
- Easy to embed with a virus

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**

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”**

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**

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

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 to protect themselves – No USB, no DVD**

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**

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Social Engineering

- “Psychological manipulation of people into performing actions or divulging confidential information.” – Wikipedia

- **The latest and most effective tool**

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….."**

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!

Beware the Wire Transfer!

- Criminals do their research

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Beware the Wire Transfer!

- Criminals do their research

- **They may register a domain name that has 1 character different from yours**

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

Beware the Wire Transfer!

- Criminals do their research
- They may register a domain name that has 1 character different from yours
- **Email comes from a principal to a finance employee requesting a wire transfer**

Beware the Wire Transfer!

- Criminals do their research
- They may register a domain name that has 1 character different from yours
- Email comes from a principal to a finance employee requesting a wire transfer
- **This has worked MANY times!**

Physical Security

- Lock the doors!

Physical Security

- Lock the doors!

- **Lock your computer: CTRL-ALT-DEL – Lock Computer**

Physical Security

- Lock the doors!
- Lock your computer: CTRL-ALT-DEL – Lock Computer
- **Logoff your computer: Start – Shutdown – Logoff**

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**

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

Protect Your Passwords!

Logical Security

Passwords!
The single most important defense

Make them Unique

Different ones for each site, application, system

Logical Security

Passwords! The single most important defense

Make them Unique
Different ones for each site, application, system

Change them regularly!

In Windows
CTRL-ALT-DEL
“Change Password”

Logical Security

Passwords! The single most important defense

Make them Unique
Different ones for each site, application, system

Change them regularly! In Windows – CTRL-ALT-DEL “Change Password”

Make them complex

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

Logical Security

Passwords! The single most important defense

Change your passwords regularly!

In Windows – CTRL-ALT-DEL “Change Password”

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

Logical Security

Passwords! The single most important defense
Change your passwords regularly!

In Windows – CTRL-ALT-DEL "Change Password"

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

Can't remember them? Use Last Pass

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

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

Never e-mail work products to your personal e-mail account

Logical Security

Meta-data

What it is

What is the risk

Solution:

Convert to PDF or use Redaction Software

Logical Security

Check your bank accounts daily

Check your credit card accounts at least monthly

Freeze your Credit Reports

Here’s the Good News!

Here’s the Good News!

The bad guys are brutally pragmatic.

Here’s the Good News!

The bad guys are brutally pragmatic.

They like easy ‘soft’ targets and there are plenty of them.

ALPINE
BUSINESS SYSTEMS, INC.
CELEBRATING 30 YEARS 2017

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!

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

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.

ALPINE BUSINESS SYSTEMS, INC. CELEBRATING 30 YEARS 2017

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 (http*S*://) 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!

ALPINE BUSINESS SYSTEMS, INC.
CELEBRATING 30 YEARS 2017

Questions

Bill Blum

bblum@alpinebiz.com

ALPINE
BUSINESS SYSTEMS, INC.
CELEBRATING 30 YEARS 2017