How to Avoid Being a Victim of Cybercrime

Call in: 1-866-814-9555
Participant code: 1669323050
Bill Blum

ALPINE BUSINESS SYSTEMS, INC.

Celebrating 30 Years 2017

Copyright Alpine Business Systems  www.alpinebiz.com
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:
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.
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 2016, **51% 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 2016, 51% of American adults had their personal information stolen by hackers, primarily through data breaches at large companies (CBS)

Total global cost of breaches:
$2,430,000,000,000,000 Yes TRILLION!
Average cost: $3.8 million (IBM)
The Magnitude of the Threat

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

In 2016, 51% 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: 133 teams by 2018
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 Apple, Google, Microsoft, Facebook, your Internet provider, and the government know about you?
Privacy

What do Apple, Google, Microsoft, Facebook, your ISP, 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

Apple

Google

ALPINE BUSINESS SYSTEMS, INC. 30 YEARS
The difference between Microsoft, Software, Apple, and Google.
The difference between

Microsoft  Software

Apple  Hardware

Google
The difference between

Microsoft  Software

Apple    Hardware

Google   Ad Agency
Nothing is free

What you give up for free technology
Nothing is free

What you give up for free technology

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
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
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
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
2016 – Ukraine Power Grid Hack disclosed
2017 – Podesta, Swift, Equifax, many others
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
The perpetrators – Who are they?  
And why do they do it?

Well Organized Criminal Networks
Who are the Targets?
Who are the Targets?

EVERYONE!
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
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
Tools of the Trade

Viruses

Spyware

Malware
Tools of the Trade

Viruses

Spyware

Malware

Hundreds of attempts foiled every week
Tools of the Trade

Viruses

Spyware

Malware

Hundreds of attempts foiled every week

Designed to steal or corrupt data and information
Tools of the Trade

Viruses

Spyware

Malware

Multiple methods of infection
Tools of the Trade

Viruses

Spyware

Malware

Multiple methods of infection: emails, texts, web sites
98% of all email is SPAM
Infection Methods
Email using Spam

98% of all email is SPAM

Easy to create
Infection Methods

Email using Spam

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

Emails and Texts

Viruses in email attachments
Infection Methods

Emails and Texts

- Viruses in email attachments
- Viruses in texts
Infection Methods

Emails and Texts

- Viruses in email attachments
- Viruses in texts
- Links to infected web sites
1 in 8 web pages are infected.

95000 per day (Google statistic)
“Drive-by Infections”

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

Be very suspicious.

This is how Ransomware works!
“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
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
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
Spy vs. Spy has been going on forever
Spy vs. Spy has been going on forever

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

Cyber warfare is more difficult than conventional warfare
We don’t even know how to define it
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
Cyber warfare is more difficult than conventional warfare

There are “honorable” hacks:
The Chinese vs. US OPM
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
Cyber warfare is more difficult than conventional warfare
There are “honorable” hacks – The Chinese vs. US OPM
There are new, very dangerous ones: N. Korea vs. Sony
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 utilizing Behavioral Analytics**

**SIEM: Security Information and Event Management**
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!
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.
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.

If possible, tether your phone or use your own personal cellular data access point (Verizon MiFi, AT&T Velocity)
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
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
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 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…..”

How Snowden did it
Beware the Wire Transfer!

- Criminals do their research
Beware the Wire Transfer!

- Criminals do their research

- They may register a domain name that has 1 character different from yours
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
The single most important thing you can do

Change your passwords regularly!
Logical Security

The single most important thing you can do

Change your passwords regularly!

In Windows
CTRL-ALT-DEL
“Change Password”
Logical Security

The single most important thing you can do

Change your passwords regularly!

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

Make them Unique

Different ones for each site, application, system
The single most important thing you can do

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
Logical Security

The single most important thing you can do

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

The single most important thing you can do

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
Logical Security

Passwords
Regularly change them
Make them unique
Make them complex
Keep them private
Use Last Pass

Never e-mail work products to your personal e-mail account
Passwords
Regularly change them
Make them unique
Make them complex
Keep them private
Use Last Pass

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

Meta-data- What it is, what is the risk
Logical Security

Passwords
Regularly change them
Make them unique
Make them complex
Keep them private
Use Last Pass

Never e-mail work products to your personal e-mail account
Meta-data- What it is, what is the risk

Convert to PDF or use Redaction Software
Logical Security

Passwords
Regularly change them
Make them unique
Make them complex
Keep them private
Use Last Pass
Never e-mail work products to your personal e-mail account
Meta-data- What it is, what is the risk
Convert to PDF or use Redaction Software

Check your bank accounts daily
Check your credit card accounts at least monthly
Logical Security

Passwords
Regularly change them
Make them unique
Make them complex
Keep them private
Use Last Pass

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

Meta-data- What it is, what is the risk

Convert to PDF or use Redaction Software

Check your bank accounts daily, credit cards monthly

Freeze your Credit Reports
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.
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!
17 Things you can do at work and home to protect yourself and your company.

1. Backup your data! Use encryption with confidential data on laptops
2. Change your passwords, make them strong, unique, private, use Last Pass
3. Keep Anti-Virus, Operating System, Flash & Java up to date
4. Configure Anti-Virus to scan anything plugged in to your computer
5. Lock or logoff your computer
6. Never e-mail work products to your personal email account
7. Never use Flash Drives you “found” or ones given to you. Buy and use brand names only
8. Smartphones: Beware of the apps you use. Delete the ones you don’t use
9. Smartphones: Use biometrics & strong passwords. Wipe before discarding them
10. Never use public USB charging stations- Always use your own charger
11. Beware of phone scams – “I’m from the Help Desk, Microsoft, the IRS, your bank…."
12. Always convert sensitive files to PDF before sending them to strip out metadata
13. Only use secure portals (https://) when transmitting personal information
14. Never use “free” music/video sharing sites
15. Protect your wireless networks with passwords
16. 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!
17. Check your bank accounts daily / credit cards at least monthly, freeze your credit reports
Questions

Bill Blum

bblum@alpinebiz.com
How to Avoid Being a Victim of Cybercrime
OPEIU Identity Protection Benefit

www.opeiulDprotect.com
Questions?

frontdesk@opeiu.org