Dannible & McKee, LLP

ANNUAL FRAUD PREVENTION CONFERENCE

Tuesday, June 18, 2019 | 8:30 a.m. - 11:45 a.m.

TECH ADVISORS

IT Support and Cloud Management

TECH ADVISORS

IT Support and Cloud Management

Cybersecurity threats are getting stronger and coming from more directions than ever before. The consequences of cybercrimes such as data theft, ransomware and computer hacks can be staggering, from the loss of customer data and other protected information to the costs associated with strengthening an infrastructure's security and repairing a damaged reputation.

How vulnerable is *your* company?

Being online in 2019 and beyond…

Today We're Going To Cover

- **The #1 security threat to your business that antivirus, firewalls and other security protocols can't protect against.**
- **Overview of Cyber-Crime.**
- **A SHOCKING truth about bank fraud that most businesses don't know about that could (literally) wipe out your bank account.**
- **9 of the Biggest Data Breaches of the 21st Century**
- **How to protect your company from Cybercrimes.**
- **Compliance with State, Federal and International Laws**
- **Written Information Security Programs (WISP)**

Ultimately, We're Going to Cover…

How to Avoid Being a SITTING DUCK To Cybercrminals and Protect Everything you've worked so hard to Achieve

About your Presenter:

Konrad Martin is a CPA and Co-Founder of Tech Advisors Inc and TA Cloud.

- Worked as a CPA for over 17 years
- Serial Entrepreneur, Konrad has owned Hotels, Restaurants, and started several small startup companies.
- Our clients benefit from our technology skills as well as our CPA background.
- We have been helping companies develop computer networks that work. I am a business consultant that concentrates on the IT needs of your company.

A Quick Overview Of The Sophistication And Proliferation Of The

Cybercrime Business

Why Cyber Crime
It's a business

Cybercrime is a 2 trillion dollar a year industry.

If you had just .1% of a slice of that pie, you'd make a cool $2 mil/year

Better question: **Why not?**

The consequences of Cyber-Crime:

Business lost during attack: Security Breaches often mean a disruption in business to the point of shutting down.

Loss of company assets: Bank account numbers and passwords stolen during a breach can cause theft of bank funds.

Damage to reputation: This is difficult to quantify but is no less real. Current and future clients rely on your reputation to maintain client records.

Litigation: The loss of PII of Clients or Employees may lead to your company being sued.

Protection Costs: It may seem like a no brainer, however most SMB's fail to implement reasonable protection methods even after a breach.

The Digital Underground's Thriving Black Market

Anyone can easily buy training, tools and services for committing fraud, hacking systems, buying stolen credit cards, setting up fake web sites, etc.

- Credit card details: $2 to $90
- iTunes accounts: $8
- Physical credit cards: $190
- Card cloners: $200-$300
- Fake ATMs: $35,000

Hackers Don't Have Rules, Regulations And Don't Have To Meet Compliance Concerns Like HIPAA, HiTech, PCI, Sarbanes Oxley, Basel III,EU GDPR, Etc…

9 of the biggest data breaches of the 21st century:

1. YAHOO – 1.5 Billion user accounts
2. Adult Friend Finder – 412.20 Million Accounts
3. Ebay – 145 Million Users compromised
4. Equifax – 143 Million Consumers
5. Heartland Payment Systems – 134 Credit Cards Exposed
6. Target Stores – 110 Million People Compromised
7. JP Morgan Chase – 76 Million households and 7 Million Small Businesses
8. Anthem Health – 78.80 Million current and former customers.
9. Quest Diagnostics – 12 Million Patients – Compromised Protected Health Information "HIPAA"

Related Posts:

- Misconfigured Webpage Exposed Patient Data
- Metrocare Services Discloses Second PHI Breach in 5 Months
- Lost Files: The Beginning of the Problems
- Ransomware Attack Shuts down Michigan Practice – Deletes All Patient Files
- Ransomware Dominated Healthcare and Small Businesses in 2018

"But We're Small...
Nobody Would Bother To Hack Us, Right?"

Wrong!

- **One in five** small businesses falls victim to cybercrime each year and that number is GROWING.
  (Source: National Cyber Security Alliance)
- Small businesses **are low-hanging fruit** because they don't believe they are a target, and therefore have very loose or no security systems and protocols in place.
- **Half of all cyber attacks** are aimed at SMBs.
  (Source: Forbes Article, "5 Ways Small Businesses Can Protect Against Cybercrime")

The Three Ways Cybercriminals Use to Gain Access to Your Files.

Internet threats are very sophisticated and involve greater knowledge in order to prevent them. Cybercriminals use three basic things to gain access to your personal information.

Online Scammers send Spam or Pop-up messages to you and try to get you to provide personal information

Email Scam Offers, detailed sales pitches, links to informational web sites. These seemingly harmless e-mails are actually the makings of an Internet crime.

Spyware is software installed on your computer without your consent to monitor or control your computer use.

How does a computer get infected with a virus or spyware?

There are dozens of ways a computer can become infected with spyware, viruses, and other malware.

- Accepting without reading
- Downloading any infected software
- Inserting or connecting an infected disk, disc, or drive
- Visiting unknown links
- Not running the latest updates
- Pirating software, music, or movies
- No antivirus spyware

The number one way to get infected is:

E-mail

As a general rule, do not open e-mail you were not expecting to receive. Computers can become infected when users open e-mail attachments that contain malicious code.

Even if the message is from a co-worker, friend, or family member, always use caution before opening a link or downloading an attachment.

This is to notify all Office 365 user that we are validating active accounts.Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely
IT Help Desk
Office of Information Technology
Office 365

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin

Send $300 worth of bitcoin to this address:

About bitcoin

Bank Fraud:

FDIC Does NOT Protect You From Bank Fraud; And The Bank Is NOT Responsible For Getting Your Money Back!

Tips For Protecting Yourself:

Cancel your debit cards; they are the #1 way bank accounts get compromised.

Have a dedicated PC for online banking and DON'T use that PC for accessing any other web sites, e-mail access, social media sites or for downloading files and applications.

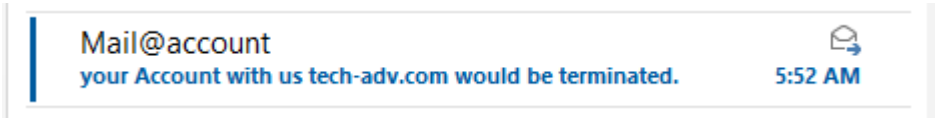
Sign up for e-mail alerts from your bank whenever a withdrawal over $100 happens.

Require YOUR signature for any wire transfers.

Have your money spread out in multiple accounts to minimize the risk.

What is your company's biggest weakness in the Fight against Cyber Crime?

YOU!



Delete | Respond | Quick Steps | Move | Tags | Editing | Speech

M

Thu 6/6/2019 5:52 AM

Mail@account <go@solikgroup.com>

your Account with us tech-adv.com would be terminated.

To Info

You forwarded this message on 6/6/2019 6:56 AM.

HI info,

tech-adv.com MAIL!

Your email account with us has been compromised since after our last mail to verify your (info@tech-adv.com) .

If you do not verify your (info@tech-adv.com) your Account with us tech-adv.com would be terminated.

Note: Verification is free and verification failed will lead to email account suspension or final termination of your mail (info@tech-adv.com) .

Click here to Verify Now to Avoid Being Terminated >>>

Thank you for your support

This E-Mail was automatically scanned for viruses

Delete | Respond | Quick Steps | Move | Tags | Editing | Speech

M

Thu 6/6/2019 5:52 AM

Mail@account <go@solikgroup.com>

your Account with us tech-adv.com would be terminated.

To Info

You forwarded this message on 6/6/2019 6:56 AM.

HI info,

tech-adv.com MAIL!

Your email account with us has been compromised since after our last mail to verify your (info@tech-adv.com) .

If you do not verify your (info@tech-adv.com) your Account with us tech-adv.com would be terminated.

Note: Verification is free and verification failed will lead to email account suspension or final termination of your mail (info@tech-adv.com) .

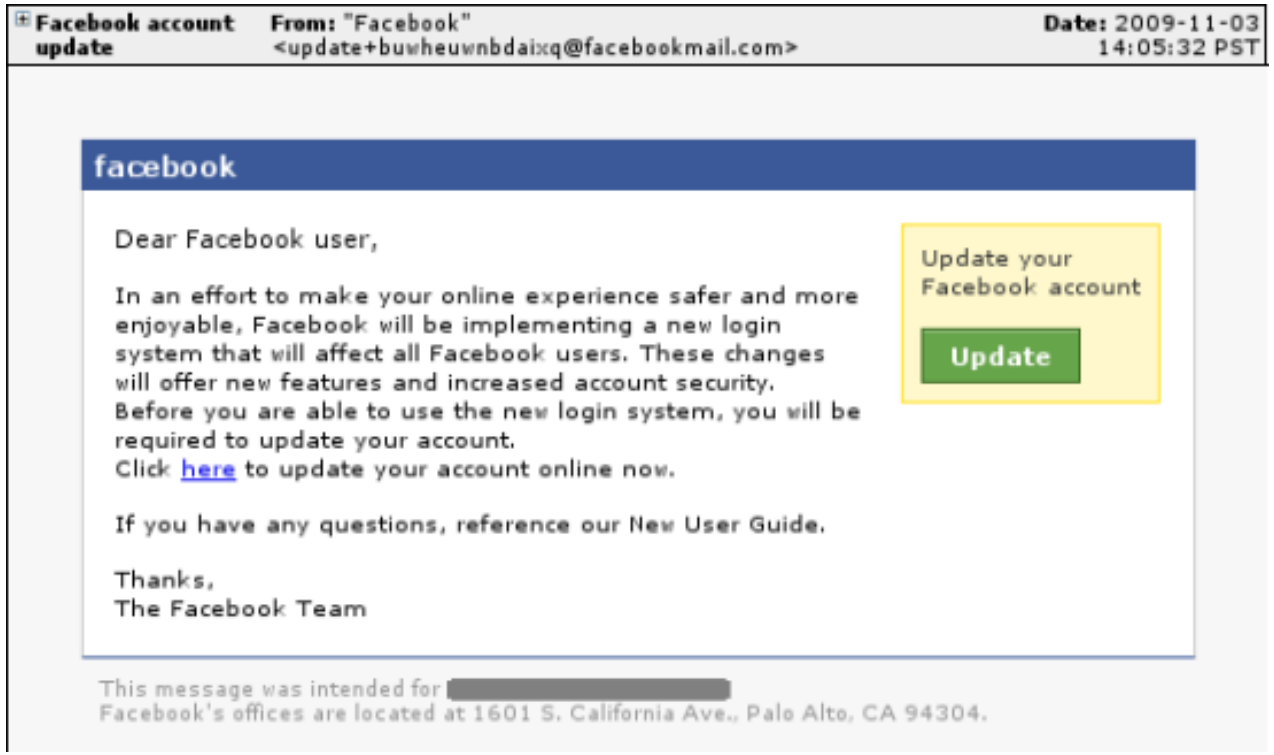
Click here to Verify Now to Avoid Being Terminated >>>

Thank you for your support

Social Media

Threat #1: Security

600,000 Facebook Accounts Are Hacked Every Single DAY.

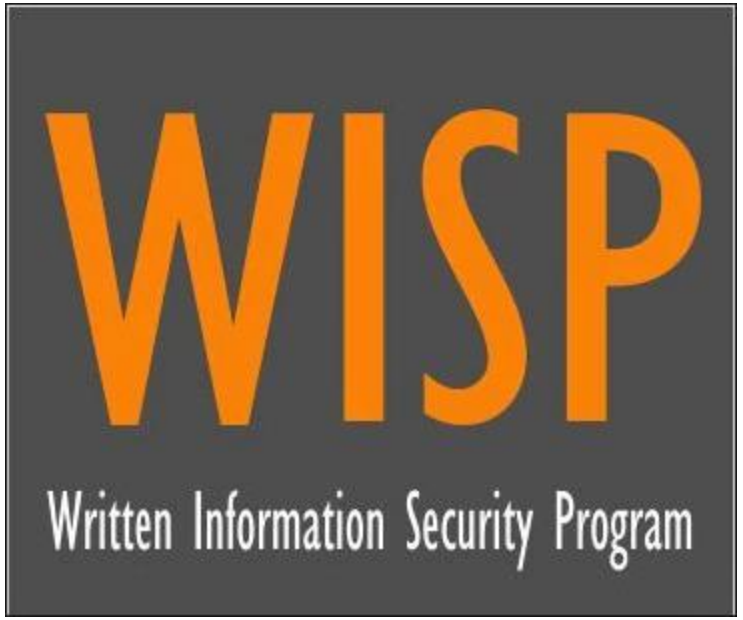


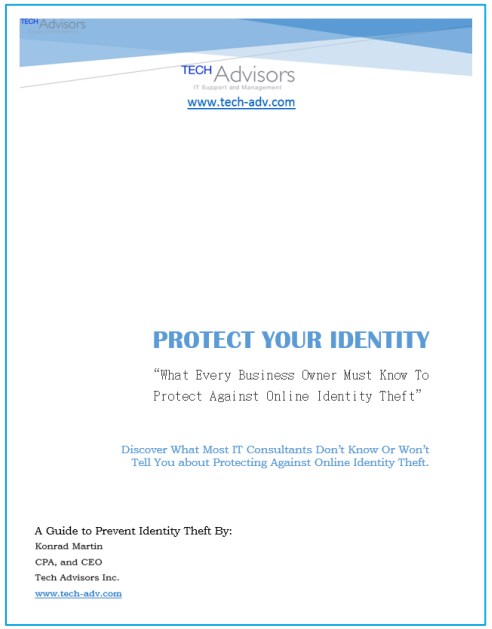
82,000

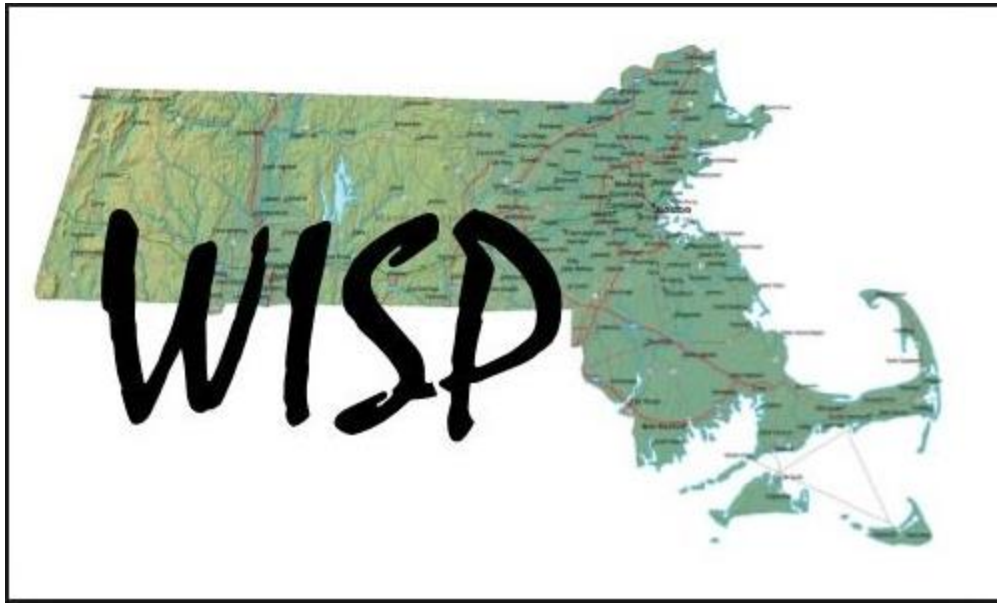
NEW Malware Threats Are Being Released *Per Day*

Source: PC World

Written Information Security Program







Things you Should Do NOW!

4 THINGS YOU SHOULD DO RIGHT NOIW TO PROTECT YOUR USER ACCOUNT IN CASE IT GETS HACKED

Last year, the top 15 hacks compromised more than 2.5 billion user accounts. You can safely assume that, even if you haven't been notified, it's likely your data is out there as well. So, get savvy and follow these simple tips.

1. Enlist in protection. In the wake of these high-profile breaches, many companies have extended free credit and identity monitoring as an olive branch to stave off lawsuits. Take advantage of it. Even if it's not free, it might be worth investing in.

2. Close loose ends. Only make an account for sites you actually visit regularly. Use guest accounts whenever possible, and delete accounts you never use.

3. Use a password manager. Seriously, most people's passwords are an absolute joke.
A password manager allows you to use a different, powerful and unique password for every account you have while still being able to remember it.

4. Freeze your credit. If you have been notified of a breach and you're worried, you can take drastic action and set up a credit freeze with each credit agency you work with. Alternatively, you can just set up a free fraud alert. *Inc.com, 12/11/2018*

TOP TIPS TO PROTECT YOUR BUSINESS FROM SOCIAL ENGINEERING ATTACKS

Every year, millions of attacks are successfully carried out against businesses just like yours. It's important to know what you're up against and how to protect yourself.
The most common social engineering tactic is phishing, often coupled with a strategy called pretexting. By gaining the trust of the victim, hackers are able to lure them into giving out sensitive personal information. Also be on the lookout for baiting, in which attackers offer free downloads, such as movies or e-books, and demand personal information from the victim. The best tools against phishing are online filters that automatically detect phishing scams, security programs, antivirus programs and education on best online practices. It should be obvious to your employees that giving out personal or company information is something they should never ever do outside of trusted sites that they can confirm are genuine. *SmallBizTrends.com, 2/28/2019*

All 50 States have Personal Data Breach Laws!

All 50 states plus the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have implemented rules requiring notification to individuals when their personal information (PI) has been compromised

Table of Contents (All 50 States)

Alabama	Alaska	Arizona	Arkansas	California
Colorado	Connecticut	Delaware	Florida	Georgia
Hawaii	Idaho	Illinois	Indiana	Iowa
Kansas	Kentucky	Louisiana	Maine	Maryland
Massachusetts	Michigan	Minnesota	Mississippi	Missouri
Montana	Nebraska	Nevada	New Hampshire	New Jersey
New Mexico	New York	North Carolina	North Dakota	Ohio
Oklahoma	Oregon	Pennsylvania	Rhode Island	South Carolina
South Dakota	Tennessee	Texas	Utah	Vermont
Virginia	Washington	West Virginia	Wisconsin	Wyoming

In General, You are subject to PI data breach laws if:

You hold a Person's name in combination with

- Driver's license number
- Social security number
- State identification card
- Financial account information and or login information

Some States & the EU GDPR defines personal information as:

- Any information concerning a data subject that can identify that subject, including:
- Names
- Number
- Symbols
- Marks
- Or other identifiers

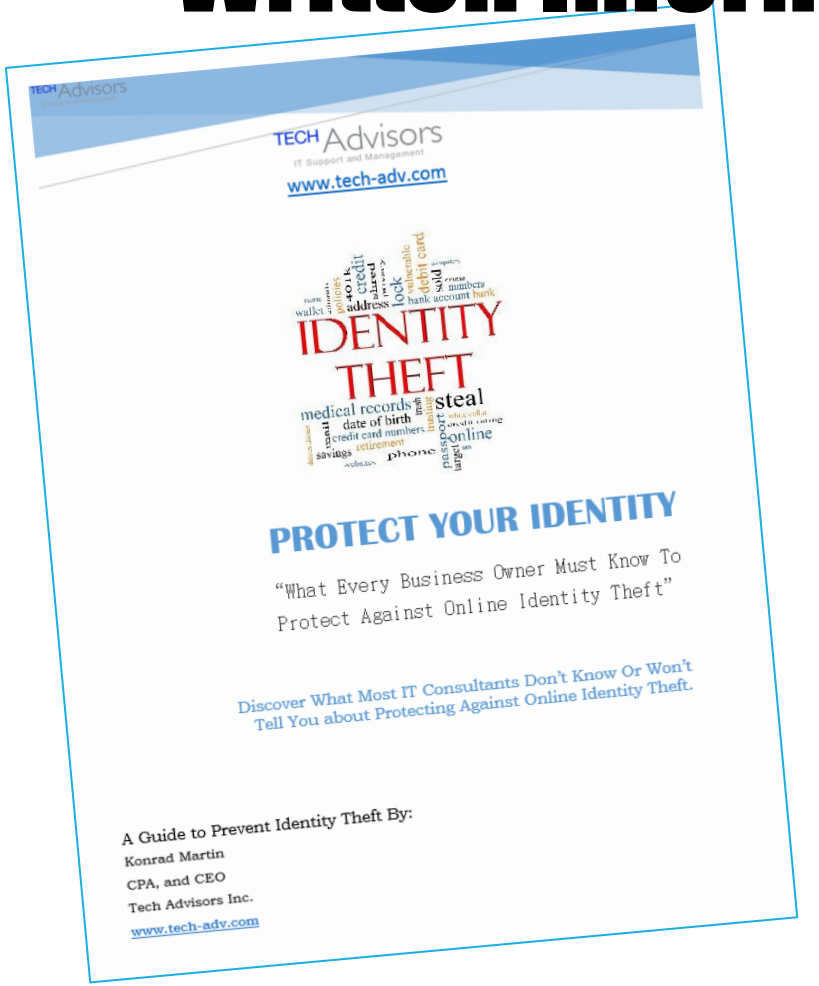
Other Laws and Regulations such as HIPAA, EI GDPR, PCI, CalOPPA (Privacy Laws) etc.

These Laws and Regulations all have their own purpose and are trying to protect certain information according to their needs.

Bottom line is, Data Breach Laws require you to have a Written Information Security Program so that you actually have Written Policies that you can conform to.

WISP

Written Information Security Plan



Gets you into Compliance and identifies weaknesses in your IT and your overall Business Process