LEGAL FIELD
– IT SPECIALISTS –

LEGAL TECHNOLOGY TIMES

"Insider Tips To Make Your Law Firm Run Faster, Easier And More Profitably"

Digital Forensics Investigation Services

With a premier team of cybersecurity professionals and a network of superb digital investigators Legal Field IT Specialists LLC offers NW Georgia law firms unparalleled confidential forensic investigation services to aid in the gathering of data pertinent to ongoing cases.

Contact Us Today at
(678) 926-9192
to receive more information about our Digital Forensics Investigation Services.

March 2020

Robert Finley, CEO
Legal Field IT Specialists

Tailored to support the needs of aggressively growing law firms, Legal Field IT Specialists has over 35 years of experience working with legal professionals. Our team is responsible for the successful technical operations of law firms throughout the southeast.

5 Signs You're About To Get Hacked — And What You Can Do To Prevent It

Hackers love to go after small law firms. There are many small firms to choose from, and many don't invest in good IT security. Plus, many firm partners and staff members have bad cyber security habits. They do things that increase their risk of a malware attack or a cyber-attack. Here are five bad habits that can lead to a hack and what you can do to reduce your risk.

1. Giving out your e-mail Just about every website wants your e-mail address. If you share it with a vendor or e-commerce site, it's usually not a big deal (though it varies by site – some are more than happy to sell your e-mail to advertisers). The point is that when you share your e-mail address, you have no idea where it will end up – including in the hands of hackers and scammers. The more often you share your e-mail address, the more you're at risk and liable to start getting suspicious e-mails in your inbox.

If you don't recognize the sender, then don't click it. Even if you do recognize the sender but aren't expecting anything from them and do click it, then DO NOT click links or attachments. There's always a chance it's malware. If you still aren't sure, confirm with the sender over the phone or in person before clicking anything.

2. Not deleting cookies Cookies are digital trackers. They are used to save website settings and to track your behavior. For example, if you search for a product, cookies are logged in your browser and shared with ad networks.

Continued on pg.2

Continued from pg.1

This allows for targeted advertising. There's no good way to tell who is tracking online. But you can use more secure web browsers, like Firefox and Safari. These browsers make it easy to control who is tracking you.

In Firefox, for example, click the three lines in the upper right corner, go into the Options menu and set your Privacy & Security preferences. Plus, every web browser has the option to delete cookies – which you should do constantly. In Chrome, simply click History, then choose "Clear Browsing Data." Done. You can also use ad-blocking extensions, like uBlock Origin, for a safe web-browsing experience.

3. Not checking for HTTPS Most of us know HTTP – Hypertext Transfer Protocol. It's a part of every web address. However, most websites now use HTTPS, with the S meaning "secure." Most browsers now automatically open HTTPS websites, giving you a more secure connection, but not all sites use it.

If you visit an unsecured HTTP website, any data you share with that site, including date of birth or financial information, is not secure and transmitted in clear-text. You don't know if your private data will end up in the hands of a third party, whether that be an advertiser (most common) or a hacker. Always look in the address bar of every site you visit. Look for the padlock icon. If the padlock is closed or green, it's secure. If it's open or red, it's not secure. You should immediately leave any website that isn't secure.

4. Saving passwords in your web browser Browsers can save passwords at the click of a button. Makes things easy, right? Unfortunately, this method of saving passwords is not the most secure. If a hacker gets your saved passwords, they have everything they could ever want. Most web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this if given the chance.

Protect yourself with a dedicated password manager! These apps keep passwords in one place and come with serious security. Password managers can also suggest new passwords when it's time to update old passwords (and they remind you to change your passwords!). Dashlane, LastPass, and 1Password are good options. Find one that suits your needs and the needs of your business.

5. You believe it will never happen to you This is the worst mentality to have when it comes to cyber security. It means you aren't prepared for what can happen. Law firms who think hackers won't target them are MORE likely to get hit with a data breach or malware attack. If they think they are in the clear, they are less likely to invest in good security and education for their employees.

The best thing you can do is accept that you are at risk. All small businesses are at risk. But you can lower your risk by investing in good network security, backing up all your data to a secure cloud network, using strong passwords, educating your team about cyberthreats and working with a dedicated IT company. Good IT security can be the best investment you make for the future of your law firm.

> **"Good IT security can be the best investment you can make for the future of your law firm."**

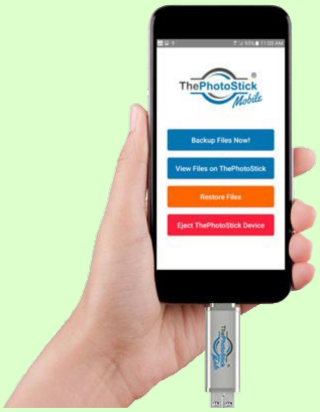
Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Law Firm Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your law firm's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you since almost all of the firms we've done this for discover they are completely exposed to various threats in a number of areas.

To Get Started And Claim Your Free Assessment Now
Call Our Office at 678-926-9192

Shiny New Gadget Of The Month:



ThePhotoStick Mobile

Never worry about running out of memory on your smartphone again! It happens to all of us – you're trying to take a picture or record a video and you get a message saying your phone's storage is full. You don't want to buy another new smartphone, so what can you do besides delete old photos?

This is where ThePhotoStick Mobile comes in. It's a memory stick compatible with most Android and iPhone devices and will boost your phone's memory without your having to buy a new phone. ThePhotoStick Mobile is an insurance policy against lost photos and videos.

ThePhotoStick Mobile gives you more control. While most smartphones work without a hitch for years, you never know if something might happen or if you'll run out of memory. ThePhotoStick Mobile plugs into your device and allows you to copy photos over. You can keep them on ThePhotoStick or transfer them to another device. Learn more at GetPhotoStickMobile.io!

Who Is Responsible For Your Corporate Culture?

"Corporate culture" is the fundamental character or spirit of an organization that influences the loyalty and general behavior of its employees. When you learn how to combine the right corporate culture with the right core values, your organization will thrive regardless of the challenges it faces.

One problem I see in most companies today is they create a mission statement only because it's fashionable to do so … but they stop there. Some may even go so far as to create a list of core values to help guide their leadership and employees … but they fail to follow them. I see lots of mission, vision and value statements on corporate websites, but the majority of employees in any company cannot recite any of them.

Several months ago, one of my clients wanted me to work with their senior management team to identify ways they could create better employee engagement. An anonymous survey was conducted, and it turned up some alarming comments. Over 50% of their employees stated that the company:

- Isn't results-oriented
- Doesn't celebrate accomplishments
- Doesn't have training for growth
- Doesn't allow them to generate ideas
- Isn't empowering them
- Has leaders who play favorites
- Has leaders whose actions do not match their words
- Doesn't involve them in the decisions that affect their jobs
- Doesn't keep them informed about changes or important issues

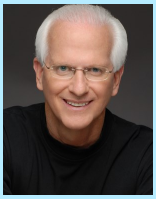
This company has five excellent "Guiding Principles" (core values) that address all these issues, but they weren't being followed. What most companies don't understand is that their "corporate culture" is in the hands of local middle management. In other words, your corporate culture is your LOCAL BOSS. They are responsible for making sure your guiding principles, core values, and mission and vision statements are being followed.

Last week I did a program for Herr Foods. Herr Foods understands the importance of living their core values. They have been in business for over 70 years and have over 1,500 employees. Their formula for success is based on the acronym L.O.V.E., which stands for:

L - Live
O - Our
V - Values
E - Every day

A recent Gallup poll found that only 34% of workers are committed to their company and are enthusiastic about their work. That means 66% are NOT engaged; they are just going through the motions, collecting a paycheck. As you look to the future, recognize that the principles that are instrumental to your success must be communicated throughout your organization on a constant basis. They should not only be part of your new employee training; they should also be part of every meeting, deeply rooted into every decision you make.

When your corporate culture is right, employees working for you no longer have jobs; in their minds, THEY HAVE CAREERS.



Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Anthony Robbins, Tom Peters and Steven Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

Don't Make This Critical Mistake In Your Business

Upward of 41% of companies don't train their HR staff on data security. This is from a recent survey from GetApp. On top of this, 55% of HR staff don't see internal data security as an issue.

HR departments often handle sensitive data and should take IT security very seriously. If a hacker were to get ahold of employee data, it could be potentially devastating to affected employees and to the company as a whole – and it could set up the company for a major lawsuit on the part of the employees.

The liability by itself isn't worth it and neither is taking on the risk by not investing in data security. Data protection needs to be in place – along with employee training. Everyone, including HR, should be on the same page, and every company should adopt strong data security and policy to go along with it. *Small Business Trends, Nov. 30, 2019*

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winner of last month's Trivia Challenge Quiz is Stuart Benning of Atlanta! He was the first person to correctly answer my quiz question from last month, the answer was: **D) Sir Tim Berners-Lee**

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 gift card to Amazon.com. Ready? Call us right now with your answer!

What computer virus replicates itself, shutting down the computer system in the process?

A) worm
B) botnet
C) Trojan Horse
D) back door

Call us right now with your answer! 678-926-9192

Follow This One Rule When Sending E-mails

We all use e-mail, and we all spend too much time reading and responding to these messages (one estimate cited by Inc. suggests the average office worker spends 2 1/2 hours per day reading and responding to e-mails). Wasn't e-mail supposed to save time? It can if you follow one important rule. It's all about streamlining your process. That rule? The CC rule.

It works like this: If you expect a reply from a recipient, you put their name in the "to" field. If you want to add more people to read your message but don't need a reply from them, put them in the "CC" field.

However, for the rule to work, everyone in the e-mail has to know how it works. If the e-mail is addressed "to" you, respond. If not and you're just CC'd, do not respond. *Simple. Inc., Dec. 10, 2019*