"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

Dan Foote
Owner/President

What's Inside:

Got IT Problem? - Click Here!

The FTC Safeguards Rule
And Your Business

FTC Safeguards Rules

The new FTC Safeguard rules require financial institutions under FTC jurisdiction to establish, enforce, and maintain an **information security program**, in writing, to protect their customers' private information.

These rules pertain not only to the information of the customers you deal with directly, but also those you deal with indirectly, through other institutions.

While it's true the new regulations provide a higher level of comfort to the general public, they also add complications to the life of a business owner.

As the leader of a business affected by these guidelines, you may feel confused and uncertain about these new regulations, or maybe you're just unsure exactly how to put them into practice in your organization.

The experts at DanTech Services offer their wisdom below on the best ways to protect your customers and get your business into compliance with the latest federal mandates. DanTech Services can also provide guidance to remedy any cyberbreaches that may have already occurred.

The latest FTC-regulated Guidelines go into effect **June 9, 2023**, that lay out the specifics for an information security program. Let's take a closer look at what a reasonable **information security program** includes:

Common IT Problems: Is Your Business At Risk?

Poor (or nonexistent) Network Security

Network security is considered one the most critical parts of keeping your business safe, along with avoiding common IT problems that little or no network security could bring.

Having a safe and secure network is important for any sized business, even if your company only has 5 employees. Hackers don't discriminate when it comes to attacking your business files and employee data. Sometimes, cybercriminals specifically target small businesses because they know a smaller business might not have a robust security policy or can be breached with as little as a friendly phone call to your staff.

Cybersecurity is something to be proactive about, and you can take many steps to ensure your network and technology devices are safe and secure.

Make sure your employees are well-trained in security principles, your company's firewall is enabled, all company data is backed up, and you're maintaining the upkeep of your passwords.

Lack of Professional or Qualified Experience

Ever heard of Managed IT Services? Just because you outsource your managed IT services doesn't necessarily mean you have to get rid of some of the members of your IT department. It may just mean those employees can focus on less technical issues that might be overly-complicated or overwhelming for them to tackle on a day-to-day basis.

An experienced and knowledgeable managed IT services provider can efficiently assist and monitor email and web hosting, data storage, server, and network maintenance, and much more. A managed IT services professional monitors and works on your most complicated IT issues. They free up your in-house staff, allowing them to tackle new projects. They also create new initiatives that can improve your business operations.

What is Trello, and how can it help me?

If you're looking for a tool for task and project management for your personal or business life, Trello might be the answer. This software allows you to collaborate with others, manage projects and deadlines from anywhere, or simply keep up with your personal To Do list.

Because of its simple, to-the-point design, Trello is known as being one of the fastest tools to learn as soon as you start working with it. Trello can help you get a "big picture" view of the tasks facing you, their deadlines, and who is working on each aspect.

For this reason, Trello is recommended to individuals or those with a small team, especially for those who might get easily overwhelmed by the complications of rapidly changing

technology, or a small team that's new to working together on a project.

A common metaphor is used when discussing project management: they say if you're going to eat an elephant, it's only possible to do so one small bite at time. Trello does this by helping you break your projects down into more manageable tasks using a system of columns and cards.

The cards are like Post-It notes that you can use to write an individual task on. These cards can be labeled with the type of task and even color-coded. And they can be moved up or down the list as your priorities change.

When you start up Trello, you'll be faced with three columns. Starting on the left is your "To-Do" list; when you start working on the task, move the corresponding card one column to the right into your "Doing" column; and once you've completed the task, move it right another column to your "Done" list.

Ambitious users find it therapeutic to see the "To Do" column shrink as the "Done" column grows.

Other handy features include the following:

- Lots of templates available, such as Business, Project Management, Personal Goals, Workflow Goals.

- A "Butler" automation tool that allows you to set up automatic systems to cut down on repetitive tasks.

- Easy integration with programs such as GoogleDocs, Google Handler, and MailTrim.

The primary cons to using Trello are that it doesn't have built-in Task Dependency management (which would allow you to keep up with which tasks can only be done once another is completed), and Trello may be too limited to handle full project management needs.

But if you're just looking for a simple way to save time, stay organized, and set/manage your goals, try out the free version of Trello, and let the program help you make sense of your projects.

Shiny New Gadget Of The Month:

Ring Always Home Drone Camera

The latest addition to Ring's suite of smart home security devices is an autonomous drone designed to patrol your property, enabling you to have eyes on places that static security cameras just won't reach.

First teased back in 2020, the Always Home drone cam was finally shown in prototype form at this years' CES.

Although there are still no concrete details of when it will be available, reports suggest that it will cost around $250, which seems quite affordable for such a high-tech piece of home security gadgetry. As well as potentially alerting you to intruders, it could also come in handy for forgetful homeowners wanting to check that they didn't leave the kitchen stove on or the windows open.

Security on Command

Left a window open or the stove on? Create flight paths ahead of time so you can manually check in with the Ring App from anywhere.

Or When It's Triggered

If your Ring Alarm1 contact sensors or motion detectors are triggered, Always Home Cam can automatically fly to see what's happening.

Privacy-Forward Design

Always Home Cam is blocked when docked and only records when it leaves the dock to fly on a preset path customized by you.

Test Your Email Security

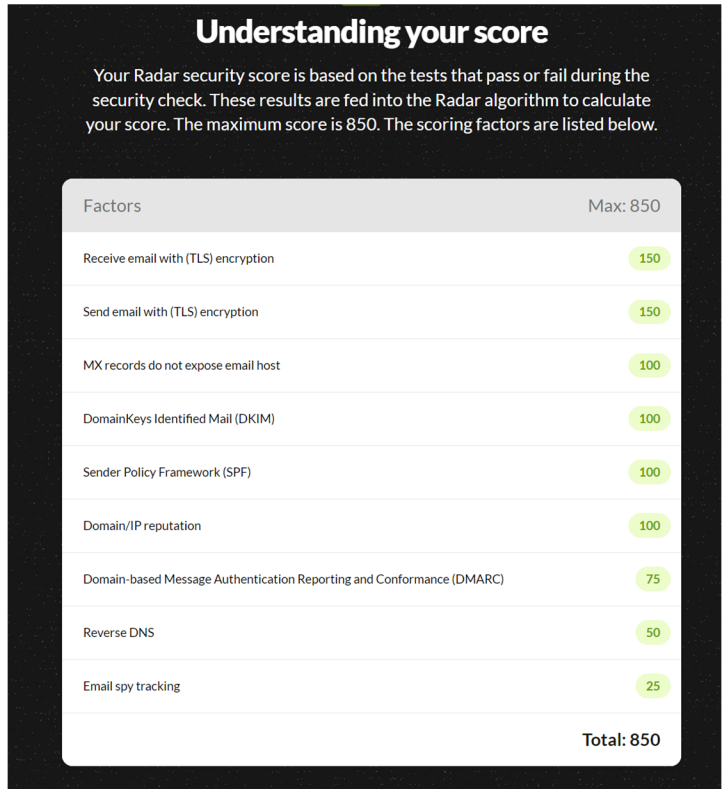Mailprotector provides a great tool to test your email security. Go to: https://email.security/radar

We encourage you to test yours. It's a simple process that asks for your email address, which sends you an email to which you simply reply.

Here on the right is the result on my email account:

We can protect your corporate email service to the same level.

Call 907-885-0501 or email me to get more information.

This is security that provides real world protection.

Dan Foote

Understanding your score

Your Radar security score is based on the tests that pass or fail during the security check. These results are fed into the Radar algorithm to calculate your score. The maximum score is 850. The scoring factors are listed below.

Factors	Max: 850
Receive email with (TLS) encryption	150
Send email with (TLS) encryption	150
MX records do not expose email host	100
DomainKeys Identified Mail (DKIM)	100
Sender Policy Framework (SPF)	100
Domain/IP reputation	100
Domain-based Message Authentication Reporting and Conformance (DMARC)	75
Reverse DNS	50
Email spy tracking	25
Total: 850	

GA4 is a new kind of property designed for the future of measurement:

Collects both website and app data to better understand the customer journey

- Uses event-based data instead of session-based
- Includes privacy controls such as cookieless measurement, and behavioral and conversion modeling
- Predictive capabilities offer guidance without complex models
- Direct integrations to media platforms help drive actions on your website or app

On July 1, 2023, standard Universal Analytics properties will no longer process data. You'll be able to see your Universal Analytics reports for a period of time after July 1, 2023. However, new data will only flow into Google Analytics 4 properties. Learn more

This property will stop processing data starting July 1, 2023

To continue collecting data, go to Setup Assistant to migrate your property to Google Analytics 4. Otherwise, one may be created for you based on your current settings. Learn more about UA deprecation

Days	Hours	Minutes	Seconds
33	04	36	53

No thanks   Go to Setup Assistant

Common IT Problem – continued

The Downfall of Old Technology

There's nothing worse than having your old and slow-working IT systems fail and not having the resources to fix them because of how out-of-date they are. One of the best ways to resolve a common IT problem, such as old technology, is the implementation of new technology as well as the fast installation of this technology.

It's important that either you or your IT team begin tackling your IT projects the second you receive new devices or the money to purchase them. A managed IT team is an excellent resource for your company as they're always looking for new and updated technology the second it comes out on the market. The more updated and newer your IT systems are, the fewer IT problems you'll have now, and in the future.

No Mobile Device Action Plan

Mobile devices (business or personal), such as smartphones and tablets, can, unfortunately, create significant security and management challenges, especially if they hold confidential information or can access your corporate network. With as much remote work we all do nowadays, a mobile device plan is pretty imperative when assessing common IT problems.

Make sure you require all mobile users to password-protect their devices (change them regularly), encrypt their data, and install security apps. This helps prevent criminals from stealing information while the mobile device is on public networks. Since these devices are portable, be sure to set reporting procedures for lost or stolen devices and communicate this to your staff.

Poor Judgement of Online Safety

Ever see something like this?
"CONGRATULATIONS! You're the 1,000,000 visitor to our website! Click here to claim your prize of $1,000,000!"

We hate to break it to you, but you didn't win. Advertisements like this are ripe with malware and other software that puts your computer at a high-security risk.
Learning how to judge the relative safety of a website helps avoid those that may harm your computer. The reason that these types of email offers exist because they work. The amount of scams taking place every day on the internet is frightening, but also something you can prevent by being cautious of the sites you visit and the information you release.

Designation of a qualified individual to oversee the program - This supervisor will take ownership and be responsible for establishing, enacting, and enforcing this program, as well as reporting regularly (at least annually) to the Board or a similar governing body. This individual can be an employee of your company or can work for an affiliate or service provider.

A written risk assessment – When conducting your risk assessment, you should take a good inventory of all personally identifiable information (PII) you have stored, noting where you have it stored, who has access to that information, and what risks threaten the integrity of that information. All aspects of the information you retain must be explored before you can determine the best practices to secure it.

Monitored/ limited access to sensitive customer information – Your security program also should include an assessment take note of who has access to secured customer information and reevaluate often whether these employees still have a legitimate need to access it. Keep employees on the access list only if they need to have access.

Encryption of all sensitive data – Encrypt all personal information that is stored on your local network. All data that is being transmitted should be encrypted using Transport Layer Security (TLS). Even consider the additional protection of encrypted e-mails within your business.

Specialized training in security awareness – The best way to ensure your employees remain active participants in your security program is to keep them aware of cybersecurity threats and the dangers they pose. Your employees have eyes on different parts of your business, and as long as they remain vigilant and tuned in, your information security programs effectiveness will be multiplied.

Incident response and recovery plan – Hope for the best, but prepare for the worst, as the wise adage reminds us. No matter how well planned your information security plan is, there's always a chance that something may go wrong. Your company may suffer a "security incident," and you're required to have established a plan to reduce the impact it could have on your business, your employees, and your customers.

Periodic monitoring of service providers to ensure they meet security expectations – the contracts your service providers and you sign should explicitly state your security regulations and include a provision for regular monitoring and reassessment of their performance

Use of Multi-factor authentication to add an extra layer of security – For anyone accessing customer information on your company's system, the FTC Safeguards require two of the following authentication factors: a knowledge factor (for instance, a password); a possession factor (for example, an authentication code); and/or an inherence factor (for example, fingerprint). The only exception would be if your qualified Individual has approved in writing the use of another equivalent form of secure access controls.

A crucial component of this program is that it must remain active. As cyberthreats constantly evolve, your program must change to keep up. IT security is best if it remains several steps ahead. What this means to your business: hiring an IT managed services provider, like DanTech Services, can aid in checking off the above requirements.

DanTech Services can scan networks for PII (Personally Identifiable Information), secure it through encryption, improve a company's security posture, deliver needed tools for other areas of management, and assist with the policies needed to fulfill FTC Safeguard requirements. To enlist assistance with your information security program, please contact DanTech Services CEO, Dan Foote. Learn more information about the company by visiting [(dantechservices.com/managed-services)](dantechservices.com/managed-services) and completing an assessment request, call him directly at 907-885-0501 or email info@dantechservices.com.