TLC TECH BYTES

JANUARY 2015

916-441-3838
www.TLCTech.com

Don't catch the great white! How to Avoid Internet Phishing!

Nowadays it's easy for hackers to get access to your important business information. They are camping out in the digital trenches waiting for you to bite.

Despite this growing trend, many businesses continue to fail to teach employees about phishing scams, one of the most common and easiest scams of cybercriminals. Phishing scams are typically fraudulent email messages appearing to come from legitimate sources. In said emails, the user is directed to a spoofed website where they try to get the user to divulge private information (passwords, credit card information, etc). The criminals then use this information to commit identity theft. So think of getting an email from your bank, internet service provider, healthcare provider etc, that you weren't expecting asking you to update your account information and you thinking the email is legit, go ahead and complete the information form.

Types of Phishing

Spear Phishing: Phishing attacks that are directed at specific individuals, roles, or organizations are often referred to as "spear phishing." As the name implies, these attacks are pointed and attackers may go to great lengths to gather specific information in hopes of making the attack more believable and increasing the likelihood of its success.

Whaling: Whaling typically refers to a type of spear phishing that is directed towards executive officers or other high profile targets within a business.

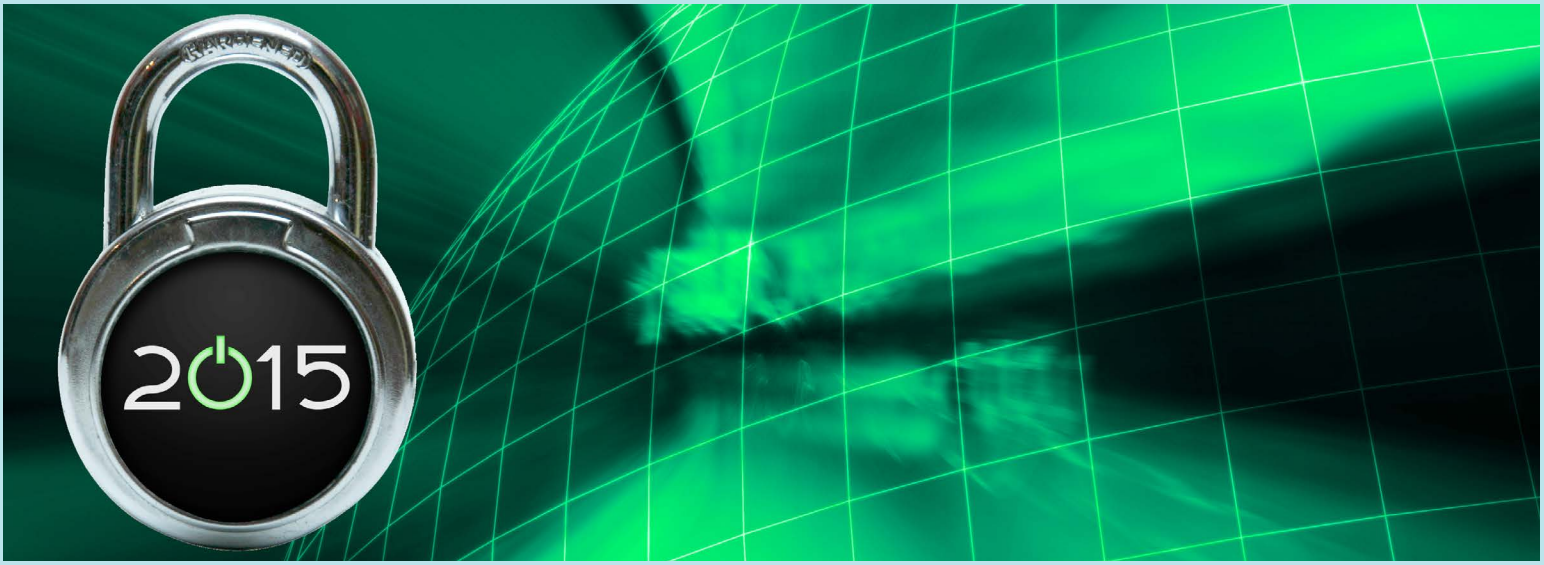
How to Avoid Phishing Scams

One of the easiest things that you can do to avoid being the victim of a phishing attack is to carefully and securely discard information (using a paper shredder or paper disposal company) that could be used in such an attack. In addition, realize that basic data about you can be relatively easy to obtain (your name, job title, favorite places or even where you bank) simply from doing a quick search online. So be leery of seemingly random requests via email or phone.

Keep in mind that most reputable organizations will not use an email to ask you to reply back with a passcode, social security number or other confidential personal information. That being said, be suspicious of any email asking you to verify or enter personal information through a website or by replying to the message itself. When you recognize a phishing email, delete the message from your inbox and delete it again from your empty items folder so that you avoid accidently accessing the websites that it points to.

To ensure that your network and inbox are safe, give the experts here at TLC Tech a call and we'll implement the security features to protect your business. Your network security is not something to be taken for granted. Catch these cybercriminals hook, line and sinker with TLC Tech!

Tips for a Scam Free New Year



This New Year you may have resolved to exercise more, eat healthier, or further your education. But don't forget to add your resolutions to build a better business. Make 2015 the year you decide to take precautions against malware and stay scam free.

Here are some tips to keep scams to a minimum in 2015!

1. Create strong passwords:
An effective password should be complex, filled with numbers, symbols and mixed-case letters to make it more difficult to crack. Avoid including personal information like your phone number or name as these can be easily searched. Instead, try using a phrase that only you know and make it related to the particular website that you are logging into. For example, if you are making a password for your financial institution, you could try a phrase like "I check my bank account daily to see what Uncle Sam has taken" and then use shorthand to recreate. So one variation could read "IcmBA1adTswU$hT."

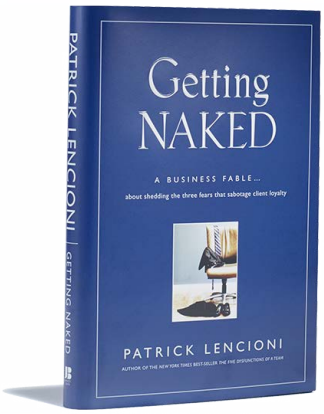
2. Update your anti-virus:
Viruses change regularly and that means that hackers are developing new ways to access the data that you hold most dear. While most anti-virus software is effective, it is only a great defense against data threats if it is kept current. The same approach should be taken to your computer programs as well. If you're receiving Microsoft update reminders, be sure to download them and follow the on-screen instructions to keep your technology up to date and safe.

3. Protect your mobile devices:
Malware doesn't just seek out desktop users. It also targets mobile devices and tablets alike. Take the same precautions that you would on a computer such as utilizing a passcode, keeping your software up to date and being mindful of the apps that you download.

4. Realize what is too good to be true:
The old adage of if it sounds too good, it probably is too good to be true applies here. Most scams carry a sense of urgency with them, forcing you to forego the research process and act immediately. A legitimate offer will give you time and the ability to consider your options, before locking into anything. Don't allow yourself to be pressured into a commitment before doing your due diligence.

Can't get enough TLC?
Like us on our facebook page.

Business Book of the Month



It's a new year, a new month, a new you. It's time to be bold in your desires and charter a new path to your own destiny. **It's time you get naked**…at least according to bestselling author Patrick Lencioni. In his book entitled "Getting Naked: A Business Fable About Shedding The Three Fears That Sabotage Client Loyalty," Lencioni illustrates the principles of inspiring client loyalty through the power of a business story. Centered on a small consulting firm, Lighthouse Partners, the story details how the firm often beats out big-name competitors for top clients. When one such competitor buys out Lighthouse, they learn a meaningful lesson about providing value to their clients.

The author asserts that people spend the majority of their lives trying to avoid awkward situations which makes them susceptible to the **three fears that inhibit client loyalty.** These fears include: the fear of losing business, the fear of being embarrassed and the fear of being inferior.

1. The fear of losing business:

No business owner wants to lose clients or revenue, as those two interests are top concerns for most business owners. Ironically enough however, these concerns often prevent many owners from having the difficult conversations that build loyalty and trust. They are afraid of telling clients what they need to hear versus what they want to hear for fear of losing capital gains. Clients however want to work with a business that has their best interest at the forefront and their needs in mind.

2. The fear of being embarrassed:

This fear is rooted in pride. No one likes to have their shortcomings pointed out or to publicly make mistakes. Lencioni argues that naked providers are vulnerable and are willing to ask questions or make suggestions even if those questions or suggestions are arguably wrong. He asserts that clients trust naked providers because they will not hold back their ideas, hide their mistakes or edit themselves to save face.

3. The fear of inferior:

Like the one before it, this fear is also rooted in ego. Unlike the fear of being embarrassed which on centered on being wrong, this fear is centered on preserving social standing with a client. The author writes that naked providers are able to overcome the need to feel important in the eyes of their client and essentially do whatever a client needs to help the client improve—even if it means that the service provider will be overlooked or temporarily looked down upon.

The key thing to remember from Lencioni's book is that it is important to be open and honest with your customers. They rely on you to have their best interest in mind and when you put them at the forefront, you'll find that they will retain loyalty with you. Naked service begins before a client actually becomes a client and will make your business come across as more generous and less desperate during the sales process.

Client Spotlight

Since the month of January typically represents a time of rejuvenation and new beginnings, we chose to highlight one of our real estate clients in this section. J B Management is a real estate developer based out of Sacramento. They have been a TLC Tech client since 2011.

Before working with TLC Tech, J B Management was experiencing email hacking issues and their old provider found it to be a challenge to determine the source of the problem. Needing an answer, J B Management sought out TLC Tech for help and the team was able to clear up the issue rather quickly. This experience aided in making the transition to becoming a TLC Tech client that much easier because the technicians proved to be knowledgeable and friendly, will at the same time explaining their technology issues in a manner that was most beneficial to the client.

When asked about the key benefits of working with TLC Tech, J B Management mentioned the proactive nature of the team. One such time when this was apparent was when J B Management had an employee who was hesitant to update their workstation for fear that it would cause multiple follow up issues. TLC Tech got ahead of the problem and minimized follow up issues so that things ran smoothly.

"I would recommend TLC Tech, and I always speak highly of the quality of their work product. They make tech work less overwhelming and confusing."
–Myra Lanham, J B Management

Goodness, gracious, great walls of Fire!

Picture this.

You've been transported back in time to the Renaissance age in Europe. Knights and fair maidens roam the countryside and as the king, you watch them from the tallest tower of your castle. It's been a prosperous year for the kingdom and you are enjoying having the lay of the land. To celebrate, you throw a ball and invite the entire town. People clamor in from the outside and neighboring lands to join in on the festivities. You greet everyone and notice an unfamiliar court jester. This court jester appears friendly and wants to perform a trick for the crowd. You think to yourself, "what harm could be done? This buffoon is only here to put on a show." You allow the jester to proceed and the crowd chuckles from enjoyment. **You are experiencing a golden age…or so you thought.**

All of a sudden, things change. Your crops are dying. You're running out of clean water. Your townsfolk are falling victim to an incurable plague. Your kingdom is suffering, with no help in sight. How could you let this happen?, you think to yourself. Where did this ill fortune come from? Was it always hiding in plain sight? Did you let some evil wrongdoer into your castle, through your own moat?

Now, imagine this same scenario happening today in the 21st century. Your business is thriving one day. Your clients are happy and content. Your data is safe and you're really starting to see a great influx of revenue. The next thing you know, everything's gone! Your data, client files, your financial information, it's all disappeared and you can't remember what it is that you did differently. Business had been normal. The only thing that occurred out of the ordinary, was that email you received from your bank, asking you to verify your account information. It seemed legitimate to you. Nothing too far out of left field. But that was no ordinary email. **That was a virus, disguised as an email**, designed to collect your personal information and infiltrate your business network.

This story is all too common. A business is hit with a security breach and doesn't have the proper security measures in place to in business. Its customers leave and its reputation is ruined.

But that scenario doesn't happen to our clients. Utilizing the power of a firewall, which is basically a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet, TLC Tech fights the battle against uninvited guests for you. **There's no slaying of digital dragons or hacker jesters here. Rather, TLC Tech acts as your knights of the roundtable, defending your business against all foes.**