June 2019

TechTidbit.com

brought to you by Tech Experts

What Are The Newest Phishing Attacks?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Phishing is a term adapted from the word "fishing." When we go fishing, we put a line in the water with bait on it, and we sit back and wait for the fish to come along and take the bait. Maybe the fish was hungry. Perhaps it just wasn't paying attention. At any rate, eventually a fish will bite, and you'll have something delicious for dinner.

How Does Phishing Work?

This is essentially how cyber phishing works. Cybercriminals create an interesting email, maybe saying that you've won a $100 gift certificate from Amazon. Sound too good to be true? Find out! All you have to do is click the link and take a short survey.

Once you click the link, a virus is downloaded onto your system. Sometimes it's malware, and sometimes it's ransomware. Malware includes Trojans, worms, spyware, and adware. These malicious programs each have different goals, but all are destructive and aimed at harming your computers.

Ransomware encrypts all your files until you pay a ransom, but even then, there's no guarantee you'll get your data restored. Malware is all about stealing credentials, passwords, and other valuable information from your company. Sometimes it's just about destroying your data.

As cyber thieves continue to steal from people all over the world, they create new ways to do this. After all, many people have become familiar with some phishing scams so they may not work as well. The solution is to come up with new scams that are enticing - things that users may not have heard about before. The more convincing hackers can make their scams, the more successful they will be.

How Has Phishing Changed?

The entire landscape of cybercrime is changing. It used to be mostly young guys sitting in their parent's basement, trying to find clever ways to pass the time. Unfortunately, this crime has become so successful that the governments of countries are now involved. A vast majority of ransomware schemes originate in Russia. The government employs hundreds of hackers, and have teams of IT experts who work around the clock to create new and more effective hacking scams.

When hackers are backed by a government like China, they have practically unlimited resources - making them harder to stop.

What Are Some Of The New Types Of Phishing Scams?

Below, we discuss some of the most notorious cybercrimes and some new ones that are making the rounds:

Gift Cards: This scam is highly successful because typically the thieves don't ask for very much money. Many victims will go ahead and pay even if they suspect that it's a trick, just because there are only a few hundred dollars at stake. You may get a phone call from someone saying they're from a creditor or the IRS. They will speak in hostile threatening tones. They'll claim that if you don't pay up immediately, terrible things will happen - maybe your car will be repossessed. Next, they instruct you to go to a local store like Walmart and buy gift cards in the amount you owe. Once you buy them, you call the thief back and give them the numbers found on the back of the cards. Once they have these, they can use them online to make purchases.

Phishing/Ransomware: Phishing crimes have become so successful that now there are variants like spear-phishing, vishing, and smishing. These are all forms of the same ruse. A hacker will send you a very convincing email. It may say something like, "Congratulations! You've just won $100 from Amazon. Click on the link below to claim your prize."

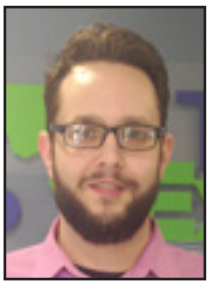
You click on the link and guess what? A malware or ransomware virus is downloaded onto your computer. If you're a business owner, this virus can spread quickly to other computers on your network. In many cases, all your computers are locked, and you'll get an ugly message saying that if you want your files restored, you must pay a ransom. Sometimes business owners follow the instructions on the screen,

Continued on Page 4

As cyber thieves continue to steal from people all over the world, they create new ways to do this. After all, many people have become familiar with some phishing scams so they may not work as well. The solution is to come up with new scams that are enticing - things that users may not have heard about before. The more convincing hackers can make their scams, the more successful they will be.

Signs Your PC Needs A Tune-Up (Or Replaced!)

"First, you really need to isolate whether your computer system is slow or if your Internet is causing the problems. This is easier than you would expect."



Jason Cooley is Support Services Manager at Tech Experts.

One of the most frustrating things a person can experience in the office is a slow computer system.

As modern systems get quicker and Internet speeds continue to soar, we really notice when performance seems off.

Watching a video online 10 years ago versus today is a world of difference. Take it back 15 years, and it's like two different universes.

Yet, we are so used to these speeds and increases in performance that we often assume that there's something "wrong" with our computer or Internet connection when it slows down. Sure, this can be the case, but how can you tell?

First, you really need to isolate whether your computer system is slow or if your Internet is causing the problems. This is easier than you would expect.

Try loading a webpage. See if there is a delay in your keyboard input. Look for spinning wheels. These are indicative of system processing actions. You can try opening a few documents or pictures stored on your computer.

If there is no delay but webpages load slower than normal, you likely are having Internet speed issues.

Let's assume that your Internet is fine. Speed is good, connection is strong. How can we tell if there is something wrong that needs fixed or if it's just a temporary issue?

Let's talk about age. The average usable life of a PC is around five years, give a take a year or two based on how good the system specs were at the time of purchase.

For instance, a laptop at a chain retail store might be a great price, but if you buy outdated products to start with, you will definitely have a harder time reaching the target goal of five years of use out of your computer. You can sometimes find a bargain, but a lot of times, you really get what you pay for.

Speaking of getting what you pay for, you may not be an expert, but remember that, while features like touchscreens are nice, they're not a great help when your system resources are maxed out.

A touchscreen in a laptop is basically a tradeoff for two other specs when it comes to cost. Basically, if you had two identically priced laptops, the one with a touchscreen would have less RAM and a slower CPU, for instance.

Other things can let you know if there is more to it than needing a new PC. Is your lag recent and sudden? How secure are you? Is your operating system up to date?

A recent virus could quickly impact your system. While they don't always work like this, a quick change in performance is typically failing hardware or an infection.

The best thing to do is to rule out the virus first. Always better to be safe. If you aren't sure about how to thoroughly check for and remove virus infections, look for someone who can help.

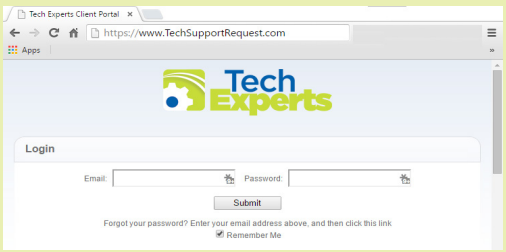
So what if you still aren't sure? If you are on the cusp of having your computer for four or five years, it might be time to make the call to replace it.

If there is a chance it's the CPU failing and it's close in the age range, replace it.

It is a calculated decision, but don't let trying to save a few bucks for a few weeks longer cause you endless frustration. It may just be time to say goodbye.

Create new service requests, check ticket status, and review invoices in our client portal:

http://TechSupportRequest.com



CFO Tech Blog: How To Become The Tech Savvy CFO

More than ever, today's CFOs are expected to have a degree of tech savviness. Big data and analytics are tools that are just too powerful to ignore in the CFO suite. If you're not particularly tech savvy, harnessing the power of these tools to the fullest extent will remain out of reach.

Why You Need to Become the Tech Savvy CFO

It's crucial to understand just how powerful today's technology tools are for financial leadership. Whatever the nature of your business and industry, technology can empower you and your staff in the following ways.

Forecasting and Risk

Forecasting has always been a part of the CFO's role. Forecasting today can be much more accurate, thanks to the rich data that's available.

CFOs must have the skills to understand and interpret that data (or they must employ people who can). Use robust data and analytics to reduce the amount of guesswork in your forecasting.

Risk management is another responsibility under your purview as CFO. Forecasting and risk management are interrelated, of course, and both have traditionally involved a fair bit of prediction and uncertainty.

If you're like most CFOs, you're a fairly risk-averse person. Reduce the risks of prediction and uncertainty by basing your decision-making on data wherever possible.

Advanced Data Visualization Techniques

All this data that companies now have access to can quickly become overwhelming. Today's tech savvy CEOs harness the power of advanced data visualization techniques to bring the most important information to the surface.

These techniques include making dashboards for interacting with the data and scorecards for presenting it to users at all levels.

Predictive Analytics

In the 1960s, business predictions were often made around a conference table in a smoke-filled room. They were based on some amount of data, but hunches, opinions, and interpersonal power dynamics often played an outsized role.

Today, there's a better way. Predictive analytics are driven by algorithms and data, not by cigars and opinions. Leverage the power of all the data you've collected into predictive analytics.

While they are neither perfect nor omniscient, predictive analytics remove human biases from forecasting. This powerful tool can enhance your effectiveness as a CFO.

Adjust in Real Time

The CFO that understands how to use these new tools can be agile, adjusting in real time based on the data that's coming in. Many marketplaces change rapidly, and a 6-month-old report may no longer ring true. Big data and analytics let CFOs make these quick adjustments as they continually monitor data and adjust their predictions.

Drive Growth

Acting on your analysis of data can often spur on innovation and growth. Creating efficiencies aids in growth, and as you do so you're likely to discover new business opportunities, such as a hole in the market that your company is suited to fill.

How to Become the Tech Savvy CFO

Having a tech savvy CFO brings many advantages to a company. As a result, being a tech savvy CFO makes you a much more valuable asset. If you're not there yet, here are a few quick tips for how to get there.

Learn Analytics

Yes, this sounds basic, but if you don't understand how to use analytics to do the things we've talked about, you need to learn. If others in your company already know analytics, leverage your rank. You are the CFO, after all—make it part of their job to teach you. If you're in a smaller firm that has yet to embrace big data and analytics, it may be time to go get a certification in this area.

Meet Regularly with Experts

Your CIO, if your firm has one, should be well versed in the sorts of technology we've discussed today. Meet regularly with your CIO and ask questions. Do the same with other experts in your network. They aren't the finance people, so they may not readily see how big data and analytics can transform your role. As your understanding grows and you learn to them the right questions, you're likely to discover breakthroughs together.

Read What They Read

Sites like CIO.com are go-to resources for CIOs, but you can benefit there, too. Not every article will apply to what you're learning, but many will. Reading sites like these will increase your overall tech comfort level.
Leverage the Data

As your understanding of analytics grows, you can start leveraging that data in real, meaningful ways. It's easy to get overwhelmed in a deluge of data if you don't have the tools to parse through it. At the same time, it's possible to parse the data so finely that you miss valuable conclusions. As your comfort level grows, you'll improve in leveraging data to the fullest extent.

Educate Your Team

Last, you need to educate your team. As you journey to become a tech-savvy CFO, teach your team what you're learning so that they can help you win using data and analytics.

"It's crucial to understand just how powerful today's technology tools are for financial leadership. Whatever the nature of your business and industry, technology can empower you and your staff in the following ways."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

What Are The Newest Phishing Attacks, from page 1

and they get their files back… but, sometimes not. There's no guarantee. Ransoms are always demanded using cryptocurrency because this form of payment is untraceable.

Wire Fraud Scam: Hackers are targeting the human resource functions of businesses of all types with phishing. They're convincing employees to swap out direct deposit banking information to offshore accounts.

A nonprofit in Kansas City (KVC Health Systems) said that there were numerous attempts each month involving scammers trying to convince their payroll personnel to change information about where to send employee pay.

The IRS recently released a warning about an uptick in a wide range of fraud attempts involving payroll information.

What Can We Do To Stop Phishing?

You may have spent years trying to build up your company. You have a huge amount of time and money invested, and yet one cyber attack could bring your company to its knees.

The first thing you need is knowledge. Knowledge is still power in our world. You need to know how cyber attacks occur. What are the latest phishing scams? How does ransomware work?

You also need to train your employees so they'll know as well. Just one careless employee can open the door to thieves and cost you thousands of dollars. It's much cheaper to invest in training your employees. Make sure your employees get regular training to remind them how to recognize a phishing email or malicious website.

Unfortunately, cybercrimes won't stop anytime soon. They've been too successful, and there's almost no chance of getting caught. What you have to do is protect yourself and your data with the best security software. If you're not sure whether your cybersecurity program is strong enough, hire a managed IT provider. They can perform penetration testing to assess your level of security.

A great managed IT service provider will do a full assessment of all your security protocols and let you know whether you need to add layers of protection. When you have the best cybersecurity platform in place, you can sleep better at night.

Using Wireless Printers? Here's How to Secure Them

With some reports estimating over seven million incidents of cybercrime and online fraud occurring in 2018, it would be a mistake to discount the risks associated with using a wireless printer.

After all, any time data is transmitted wirelessly, there is a chance it could be intercepted. When you think about all the sensitive information that is printed in your company, this threat may then seem quite real.

Try the following tips to minimize the risk of a security vulnerability associated with wireless printing:

Use WPA2

This security certification program essentially password protects your print job capabilities just as you would require login credentials to access wireless internet.

By controlling access to your wireless printers, you can also monitor who is printing what and detect when someone attempts to gain unauthorized access to your systems.

Keep Security Software Updated

Many printers come with some form of built-in security, but the installed version can only be effective for so long.

Regularly check for more updated versions of your printers' security software and install them as they become available to be protected from the latest threats.

Use Data Encryption

Just as your emails and other document sharing methods are encrypted during transmission, you should make sure your printer data is encrypted as well.

This ensures that, if the information is intercepted by a nefarious third-party, they will not be able to decode the stolen data. This is especially important for printers you use to print checks.

Train Your Staff in Printer Protocol

No matter what measures you take to secure your wireless printers, they won't be as effective if your staff doesn't know how to properly use equipment or keep protection programs up to date.

Provide training to your employees about safe printing practices.

These tips don't just apply to large businesses; the threat of a security breach through wireless printing systems can affect small businesses and even individuals just as easily.

With a little forethought and effort however, you can greatly decrease these risks to be able to print without fear.