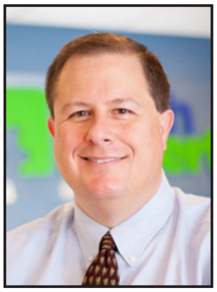
September 2020

TechTidbit.com

brought to you by Tech Experts

The Eleven Types Of Phishing Attacks You Need To Know To Stay Safe



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

Like Darwin's finches, phishing has evolved from a single tenchinque into many specialized tactics, each adapted to specific targets and technology. First described in 1987, phishing is now carried out via text, phone, advertising and, of course, email.

Boiled down, all of these tactics exist for the same purpose - to steal confidential information from an unsuspecting target in order to extract something of value.

Knowing about the hugely diverse set of today's phhishing tactics can help you be more prepared for the inevitable instance when you become the target.

Standard phishing - casting a wide net

At its most basic, standard phishing is the attempt to steal confidential information by pretending to be an authorized person or organization. It is not a targeted attack and can be conducted en mas.

Malware phishing - beware the macros

Using the same techniques, this type of phishing introduces nasty bugs by convincing a user to click a link or download an attachment so malware can be installed on a machine. It is currently the most widely used form of phishing attack.

Spear phishing - catching the big one

Where most phishing attacks cast a wide net, hoping to entice as many users as possible to take the bait, spear phishing involves heavy research of a predefined, high-dollar target - like a CEO, founder, or public persona - often relying on publicly available information for a more convincing ruse.

SMS + phishing = SMISHING - just don't click

SMS-enabled phishing uses text messaging as a method for delivering malicious links, often in the form of short codes, to ensnare smartphone users in their scams by clicking texted links.

Search engine phishing - careful what you choose

In this type of attack, cyber criminals wait for you to come to them. Search engine phishing injects fraudulent sites, often in the form of paid ads, into results for popular search terms.

Vishing - keeping you on the line

Vishing involves a fraudulent actor calling a victim pretending to be from a reputable organization and trying to extract personal information, such as banking or credit card information.

Most often, the "caller" on the other line obviously sounds like a robot, but as technology advances, this tactic has become more difficult to identify.

Pharming - poisoning the waterhole

Also known as DNS poisoning, pharming is a technically sophisticated form of phishing involving the internet's domain name system (DNS). Pharming reroutes legitimate

Continued on page 4

SMS-enabled phishing uses text messaging as a method for delivering malicious links, often in the form of short codes, to ensnare smartphone users in their scams by clicking texted links.

We're proud to partner with the computer industry's leading companies:

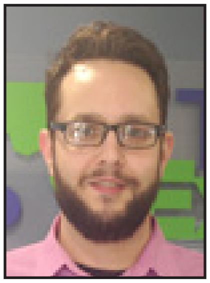
Microsoft Partner

Microsoft Small Business Specialist

Business Partner IBM

Is Your Network Stealing Your Staff's Time?

> *"We've all become so reliant on computers that we've forgotten how to perform simple tasks ourselves. And we go into panic mode when they stop doing what we expect of them."*



Jason Cooley is Support Services Manager at Tech Experts.

At some point in the last six months, maybe you've been on a Zoom call or chatting away in Microsoft Teams and wondered what would have happened if Covid had come along in the 1980s or even 1990s.

Let's be honest… the world would have totally shut down. Business would have completely ground to a halt. We couldn't have done the last six months without the amazing technology that we now totally take for granted.

Depending how old you are, what we can do easily today was literally the stuff of dreams just 20 years ago.

But as much as great IT has made working from home easier and enabled many businesses to keep going, we also must remember that bad IT can still be a massive time thief.

We've all become so reliant on computers that we've forgotten how to perform simple tasks ourselves. And we go into panic mode when they stop doing what we expect of them.

Most businesses find that even the most committed staff in the world will jump at the chance for a little bit of office down time. So, when computers aren't doing their job that's a great opportunity to down tools and do very little.

If they're in the office, people sit around chatting or go home early, while every second your business is losing money.

That's not to say that all employees want to take the easy way out. There will be others who like a challenge and want to try their best to make things better, using their own limited IT knowledge or good old Google to guide them.

Unfortunately, IT set ups are complex. And if you don't really know what you're doing you could end up digging a far bigger hole for you and your entire organization.

Well-meaning staff, no matter how lovely and helpful they might be, can cause more problems than you could ever imagine.

Just like you wouldn't want someone who did a biology class 20 years ago to perform open heart surgery on you, you really don't want someone who's just watched a couple of YouTube tutorials fixing your business's computer system.

This is what we do, day in, day out. And we're the local experts.

If you want to ensure that your workforce doesn't grind to a halt when things stop running smoothly, it pays to invest in experts who can:

a) Stop most things from going wrong in the first place, and
b) When they do go wrong, get you back on track quickly and reliably

That means minimal downtime, less chatting and more getting things done.

What Exactly Is The Cloud? And Is It Safe?

It's the kind of question you'd think would be easy to answer, until someone asks you: What exactly is the cloud?

Put simply, it's using someone else's computers over the internet to do things we used to do in our own computers. Like run software or store data.

When you run software in a tab in your browser, that software is still running on a computer… it's just not your computer. That means you can run very powerful applications without needing a powerful computer. Excellent!

So, is the cloud safe? The answer is that it depends.

While there's no technology that is 100% safe - working with the larger cloud providers is often safer than running things on your own network. Simply because they have dedicated teams of security experts.

You should also focus on making sure your business's use of the cloud is safe too.
Such as by:

- Never ever sharing logins (even amongst your team members)
- Making sure you use randomly generated passwords protected by a password manager, and
- Keeping all devices 100% up-to-date at all times with Updates and Next-Gen Anti-Virus tools

Password Security: Lock Your Digital Doors Too

Mark Funchion is a network technician at Tech Experts.

Password security may not be on the forefront of everyone's minds – but it's more important and easier than ever.

Password security issues have been going on for a long time. Back in November 2014, a webpage started livestreaming security cameras from around the world that had not updated the default credentials. In the US alone, there were over 11,000 cameras livestreaming; a year later in December 2015, there were still almost 6,000 cameras live. [CSOonline.com]

Then in December 2019, many Ring camera accounts were hacked – not with default passwords this time, but actual hacks on accounts without two-factor authentication. [vice.com]

What exactly is two-factor authentication? Two-factor authentication means a second confirmation after your password. This second method is often sent to your cell phone as a text or through an app, which you then input or confirm. Many banks require this, but there are also lots of other sites which have it as an option, like Ring.

While many people see this as an inconvenience, it is a safety feature and it's becoming the new standard for security.

A good analogy for this is a deadbolt on your door. Your door handle has a working lock, but it is not too hard to get through that lock.

As a second security method, you turn your deadbolt to make it much harder to access your home. That is your physical two-factor authentication – and if it is important enough for entry physically into your home, it should be important for virtual access as well.

Even if you do not have two-factor authentication, at least changing the default passwords and using different passwords across all your accounts are vital steps to more secure accounts. While it's very convenient to have one password for all your accounts, it also means that if one account is compromised, they are all compromised.

If a hacker gains access to an account and you use the same password for your email, they can "verify" account ownership and change your passwords to lock you out.

That's why your method of two-factor has to be secure too. If you have verification codes sent to your email and your email password is "password," that second factor is not helping. It's just a second "door" that a hacker can walk right through. Not much of a defense.

Going back to the importance of changing default passwords, most of us own a lot of devices in our house that are network-connected. And it is very easy to plug them in, take all the defaults, and go on with your day.

If you live in an area with a lot of neighbors nearby, take a look at the wireless networks you can see.

From my desk at work, I can see over ten networks that are outside of our office. The signals from unsecure devices aren't kept within the walls of your own home.

A quick Google search can tell you the default username and password of almost anything, including unsecure devices that might be in your own home. In the Symantec Internet Security Threat Report for 2019 [https://docs.broadcom.com/doc/istr-24-2019-en], 60 percent of the IOT attacks (Internet of Things – meaning everything Internet-connected) used a username of "root" or "admin" and over 40 percent of the attacks used a password of "123456" or left that field blank. Not the work "blank" – an actual password of nothing.

People almost always worry about security in some form: we lock our cars, our houses, our cell phones. The same philosophy should be applied to our technology.

Take the time to change your passwords, use varying passwords, and change them periodically. It does not take much of a hacker if we don't bother to lock our own doors.

> *"While it's very convenient to have one password for all your accounts, it also means that if one account is compromised, they are all compromised. If a hacker gains access to an account and you use the same password for your email, they can "verify" account ownership and change your passwords to lock you out."*

The Eleven Types Of Phishing Attacks, continued

web traffic to a spoofed page without the user's knowledge, often to steal valuable information.

Clone phishing

In this type of attack, a shady actor makes changes to an existing email, resulting in a nearly identical (cloned) email but with a legitimate link, attachment, or other element swapped for a malicious one.

These attacks can't get off the ground without an attacker first compromising an email account, so a good defense is using strong, unique passwords paired with two-factor authentication.

Man in the middle - the public WiFi phisherman

A man-in-the-middle attack involves an eavesdropper monitoring correspondence between two unsuspecting parties. When this is done to steal credentials or other sensitive information, it becomes a man-in-the-middle phishing attack. These attacks are often carried out by creating phony public WiFi networks at coffee shops, shopping malls, and other public locations. Once joined, the man in the middle can phish for info or push malware onto devices.

Business email compromise - don't make the payment

One of the most expensive threats facing businesses today is business email compromise. This involves a phony email usually claiming to be an urgent request for a payment or purchase from someone within or associated with a target's company.

Malvertising - that ad isn't what you think it is

This type of phishing takes advantage of exploits within advertising or animation software to steal information from targeted users.

Malvertising is usually embedded in otherwise normal-looking ads - and placed on legitimate websites like Yahoo.com - but with malicious code implanted within.

How to protect yourself from phishing

Protecting yourself from phishing attacks starts with knowing what's out there. In fact, ongoing security awareness training can help reduce breaches by nearly 70%.

Here are a few tips to keep in mind to avoid getting phished:

1. Never click on links from unknown senders or if any detail about the exchange has aroused suspicion.

2. Whenever possible, hover over a link to ensure the destination matches your expectations. Note: this will not work on mobile or if short codes are used, so be extra wary on mobile devices.

3. If you suspect an email is a phishing attempt, double check the sender name, specificity of the salutation, and a footer for a physical address and unsubscribe button. When in doubt, delete.

4. If you're unsure if a communication is legitimate, try contacting the sender, brand or service via another channel (their website or by calling a customer service line, for instance).

5. Avoid entering personally identifiable information unless you are confident in the identity of the party you are communicating with.

Do We Have A Connection Here Or What?

Most businesses are heavily reliant on the internet. Everything is cloud-based and streamed. And it's especially important now we have more people working from home than ever before.

Without the Internet, those Zoom chats wouldn't work. We'd spend the day with a mobile phone glued to our ear, and probably with chronic neck ache. Ouch.

So how do you cope if one or more of your remote workers has a poor Internet connection? That can quickly become a frustrating experience for everyone.

Your first port of call would be to run a speed test and then shop around. Find out which providers offer the best speed in their area.

And if they need to, switch. You might choose as a business to financially help them with upgrading their home Internet.

If that's not an option, then we need to get a little more creative. In extreme cases, you can look at alternatives such as satellite Internet, or a Wi-Fi router that uses 4G.

You can also check their Wi-Fi router to see if an upgrade would be beneficial. And there are things called range extenders than boost the Wi-Fi to reach different parts of their home.

If you're not sure what you're looking for or could use some advice on helping your staff get more done from home, call us.

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

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.