September 2019

TechTidbit.com

brought to you by Tech Experts

How To Protect Your Business From SHTML Phishing

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

Data security is vital to any business. Learn how SHTML phishing works and how to minimize the risk of your data falling into the hands of attackers.

Email phishing has been in the playbook of hackers since, well, email. What's alarming is the scope in which criminals can conduct these attacks, the amount of data potentially at risk, and how vulnerable many businesses are to phishing attempts.

Here's what you need to know to spot the hook and protect your data from being reeled in.

How Does Email Phishing Work?

A phishing email typically contains an attachment in the form of a server-parsed HTML (SHTML) file.

When opened, these shady files redirect the user to a malicious website often disguised as a legitimate product or service provider.

The website then requests sensitive information such as the user's address, date of birth, social security number, bank account number, etc. in exchange for providing said product or service.

Users who comply end up giving their information to a criminal who may then sell it to various illegal organizations.

Victims may end up losing money and having their identity connected to criminal activity. The attackers may even offer to sell the information back to the owner for a hefty ransom.

For businesses, the damages can be irreparable. Phishing is often the launchpad for large-scale cyber attacks, and businesses that fall victim can lose not only cash and assets, but the trust of current and would-be customers.

Who Does SHTML Phishing Target?

While many individuals fall victim to phishing, the main targets are businesses in the banking and finance sector.

The sender may use a seemingly legitimate email address, often posing as a trusted, reputable organization.

They may goad users to open attachments by claiming to be the IRS, a wealthy businessman offering a lucrative deal, or, ironically, a security provider offering to scan the user's computer for vulnerabilities.

While many phishing attempts are obvious, some can be convincing, and all it takes is a hasty click to give the phisher what they want.

Types of SHTML Phishing

Depending on the attacker, a phishing attempt can range from simple and generic to detailed and personalized to fit the target.

For businesses that conduct large quantities of transactions, a phisher may send a simple email claiming to provide a receipt for their purchase. Others may send invoices.

Sophisticated attackers may gather information about the business including its suppliers, partners, and even names of individual employees.

They may then create fake accounts disguised as these trusted entities, fooling the target into giving away sensitive data.

While most phishing attempts fail, a convincing premise combined with a busy, distracted user can equal success – and disaster.

Potential Signs of SHTML Phishing

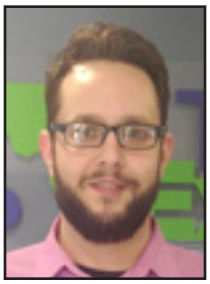
Being proactive and training your employees to spot phishing is the best line of defense. Here are some potential red flags that may, but not always, indicate that an email is a phishing attack:

Continued on page 4

While many phishing attempts are obvious, some can be convincing, and all it takes is a hasty click to give the phisher what they want.

Windows 10 Feature Updates: Changes Going Forward

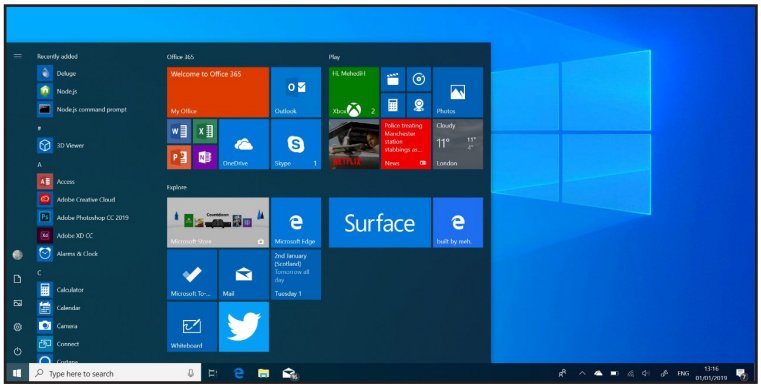
"While inconvenient, it isn't Microsoft intentionally causing you grief. To simplify it as much as possible, Microsoft makes changes they find necessary. Sometimes, those changes cause already installed software (and potentially any future installed software) to stop working."



Jason Cooley is Support Services Manager at Tech Experts.

Windows 10 and its updates have been an interesting ride to say the least. For IT professionals, like us at Tech Experts, Windows 10 updates have caused a myriad of problems in the last few years. You don't have to be a Tech Expert to have experienced some of these problems.

Over the years it has not been abnormal for Windows Updates to cause issues for users. Third party software could potentially function different or not at all after updates. Your printer may stop working. You could lose a shortcut.



While inconvenient, it isn't Microsoft intentionally causing you grief. To simplify it as much as possible, Microsoft makes changes they find necessary. Sometimes, those changes cause already installed software (and potentially any future installed software) to stop working.

These issues seem to be more prevalent in Windows 10 and there are more than a few I would classify as large scale issues. Microsoft attempts to fix issues that are reported, based on how impactful they are and how many users they affect. If a common sound driver isn't working for 50% of Windows users, that would be a priority fix.

So where do these issues come from?

Windows has different types of updates. The large updates with major changes to the system are called Feature Updates. These updates have been rolling out twice a year and in the opinion of many, this is where the issues originate.

Twice a year, your system has a good chance of having something not work correctly for an unspecified amount of time. Not a great user experience. Feature updates are intended to create a better user experience, make needed changes, or improve functionality. The broken software, drivers, or even data loss are just free bonuses.

Additionally, Microsoft has two groups for how updates are sent out. If you are a Windows Insider, you get the upgrade first and act as a live tester to eliminate the worst of these issues. Then, once Microsoft determines they are ready to deploy to the second group of users, the feature updates push all of the changes all at once, for better or worse.

Good news ahead

I have been hard on the updates because of the level of frustration caused by them for consumers and professionals alike. Thankfully, Microsoft recently announced that next year it will start a new model for its update cycles. Instead of two major feature updates every year, there will be one major and one minor feature updates per year. The schedule will include major upgrades in the spring and minor upgrades in the fall.

There are more changes to the way updates work coming as well, and I believe they will help prevent many of the problems that the updates the last two years have caused.

There are changes to the deployment model coming as well. The Insiders will still receive the updates first, but the rest of the Windows users will catch a big break here.

Instead of the major feature update coming all at once, the feature changes and upgrades will be released slowly. As Microsoft's John Wilcox notes, "we are using a controlled feature rollout (CFR) to gain better feedback on overall build quality, [so Slow Ring subscribers] may not see the new 19H2 features right away."

These last two years haven't been easy, but the new process will almost certainly save us a lot of time, alleviate a few headaches, and make for a better user experience.

Basically, what they were supposed to be doing all along.

Why Antivirus Software Is So Important

Alexander Stahl is a help desk intern at Tech Experts.

Workplaces across the world are constantly under fire from security threats stemming from computer viruses.

As businesses have updated their technology throughout the years, the implicit security that stemmed from the use of typewriters and handwritten documents has diminished.

Now, everyone is connected to their neighbor, making businesses as vulnerable as ever to fraud and theft of sensitive information. To combat it, every workplace should be well-equipped with a proven and trusted antivirus software.

A virus is a malevolent program meant to do any number of things. They can hijack your PC through phishing scams, careless downloads, and even by accidentally clicking on an online advertisement.

Overall, viruses can slow down your PC, steal sensitive data stored on your machine, prevent computers from booting up, and send out messages under your alias.

Much like real life, viruses can essentially be "contagious" and spread across a network, making them a business's worst nightmare. One infection could create a site-wide virus epidemic if it spreads across the network – and some are designed to do just that.

In addition, not all viruses are the same. The term "virus" is really an umbrella for many different types of malware.

For example, there are worms, which make an indefinite amount of copies of themselves to take over your CPU.

Trojans are seemingly good-natured programs, but in reality, they secretly perform some sort of malicious attack whether that is stealing your information or slowing down your PC.

Another example of a virus is spyware, which does not stop your PC from running smoothly, but just as the name states, it spies on your activity and collects sensitive information without your knowledge or consent.

All users need antivirus to keep themselves and their fellow coworkers safe. Antivirus acts as the security guard defending your computer. Its primary task is that of a gatekeeper. It stops viruses from attaching themselves to your workstation before they even become a threat.

Although antiviruses do a stellar job at the gate, some viruses can still slip through the cracks. In these cases, antivirus software can find and remove threatening programs from your device. Most antivirus software notifies you of the removal as well or asks for permission before fully removing the program from your machine.

In order for an antivirus software to be successful and functioning, the developers must be dedicated to updating the antivirus' database consistently with new information on new threats, so be sure to keep your program up-to-date.

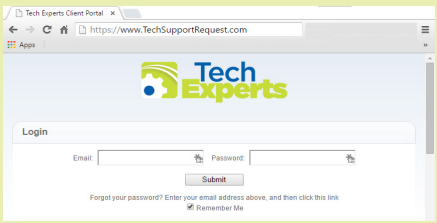
Just as the field of computer science and technology is rapidly changing and improving, so are the viruses and malware that attack your computer. Many antiviruses are consistently updating their databases and rules to account for this growing and changing threat.

Lacking antivirus software for your business is like leaving the door unlocked for hackers and malicious programs to do what they please with your costly computers and sensitive information. The best way to fight a cyberattack is to prevent it from happening in the first place, and antivirus software does just that.

"Now, everyone is connected to their neighbor, making businesses as vulnerable as ever to fraud and theft of sensitive information. To combat it, every workplace should be well-equipped with a proven and trusted antivirus software."

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

http://TechSupportRequest.com



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

The Cloud – Have You Harnessed Its Strategic Advantages?

The cloud may still feel like a new technology – but in reality, it's been around for more than 10 years now. Does that make you feel old?

Let's be clear about something – the cloud is here to stay. In recent years you may have still heard the occasional "industry insider" suggest that the world may be moving too quickly to an untested and unsure platform in cloud computing, but no more. The cloud is now an integral part of daily life for private consumer and business users alike.

What Is The Cloud?

The cloud is a network of technologies that allows access to computing resources, such as storage, processing power, and more. That's where the data is – in these data centers all around the world. Which data center your data is in depends on what cloud service provider you're working with.

The Cloud Isn't As New As You Might Think

Would you say the cloud is "new"? To some, this may seem like a question with an obvious answer, but it's not that simple. The way in which we think about technology can lead to something feeling new for a lot longer than would make sense otherwise.

After all, the cloud is more than a decade old, but a lot of people still think of it as a new technology.

You Need To Keep An Eye On Your Cloud

As beneficial as the cloud can be, it's important to note that it can also pose risks if it isn't managed properly. It all comes down to the classic binary relationship between convenience and security.

The cloud gives you unparalleled access to your data from anywhere with an Internet connection. That means that external parties (including cybercriminals) can have undue access to your data as well if you don't take the necessary steps to secure your environment.

That's why you need to monitor your cloud. No matter who you entrust your data to, you should ensure that you or someone in your organization is given appropriate visibility over your cloud environment. That way, you can guarantee that security and compliance standards are being maintained.

If you don't have the resources to manage this type of ongoing monitoring, then it would be wise to work with the right third party IT services company.

Doing so will allow you to outsource the migration, management, and monitoring of your cloud.

You'll get the best of both worlds – security and convenience.

How To Protect Your Business From SHTML Phishing, continued

- Poor spelling and grammar
- Strange characters and punctuation
- Email addresses comprised of a seemingly random combination of letters and numbers
- Emails claiming to offer large sums of money
- Emails claiming that you owe a large sum of money
- Emails claiming that your data is at risk and offering protection, usually for a fee
- An overly lengthy or short email body
- Attachments with file types you don't recognize

How to Protect Your Business from SHTML Phishing

The greatest defense is training every employee to recognize the red flags, especially the not-so-obvious ones. Make basic data security a part of the onboarding process, and hold presentations and seminars several times a year to keep employees aware and bring to light any new threats they should look for.

Data security is more relevant than ever, and businesses need to stay up to date on the latest cybersecurity threats. Is your business taking the necessary precautions to keep phishers away and protect your valuable data?