August 2015

TechTidbit.com

brought to you by Tech Experts

Wire Fraud: How An Email Password Can Cost You $100,000

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

Wire fraud is one of the most financially damaging threats to people and businesses today. Victims can lose hundreds of thousands of dollars in the blink of an eye.

What is wire fraud? Let's start with the basics:

A wire transfer is an electronic transfer of funds between entities, usually a bank and someone else. Wire fraud utilizes this system to steal money.

Typically, this is done by fooling a financial institution into wiring money to a fraudulent account.

The process often begins with the theft of personal data or email credentials, which means data security is paramount to preventing this threat.

Here's an overview of wire fraud so you can better protect your business and clients.

Wire fraud grew 10x in 10 years

Three out of four attempts of any type of fraud involves a wire transfer, according to a report from Guardian Analytics.

This is not surprising given the size of the target. The amount of money transferred across telecommunications reached $600 trillion in 2012. When there is that much money in play, scammers will always look to take advantage.

Wire-fraud attacks have increased ten-fold since 2003, according to the Wall Street Journal, and they continue to evolve to better take advantage of security flaws.

Wire fraud tactics abound

Wire transfer fraud is a complex problem. Scammers can gather information and launch attacks in a dizzying number of ways.

Most attacks begin with the theft of a victim's email credentials or enough personal data to impersonate the victim at a financial institution. The attacker then tricks the bank into wiring money to a fraudulent account and *poof*! The money is gone.

> *"Most attacks begin with the theft of a victim's email credentials or enough personal data to impersonate the victim at a financial institution."*

Attackers use methods such as malware, phishing, and social engineering to get information or email credentials. They then have an equally broad number of ways to approach the financial institution, as described in the report:

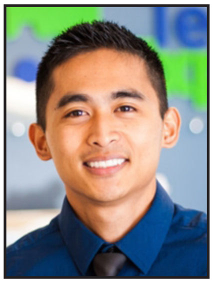
Defeat Out-of-Band Confirmation: In this scam, the attacker compromises an online bank account and removes security alerts and/or changes the contact information. Then the scammer can request a wire transfer and confirm his own request without the victim ever knowing.

Funeral Scheme: Once a victim's email account is compromised, the attacker sends an email to the victim's bank and requests funds for a funeral (or some other reason that earns sympathy). The attacker claims to be out of the country, so the bank sends a form to fill out, sign, and return. The attacker relies on the bank not carefully

Continued on Page 4

How Can Small Businesses Amplify Employee Communication?

Traditional phone systems often hinder communication effectiveness because of their limited mobile capabilities. This often results in lost money, lost productivity, and big headaches.



Michael Menor is Vice President of Support Services for Tech Experts.

Using email to conduct important business always starts with the best intentions, like saving everyone time. Just think back to the last time you used email to solve a significant business issue or answer detailed questions from an important customer.

But, sometimes, email creates a disaster of miscommunication. Tone, intonation, and emotion get lost in translation. Messages and ideas are misunderstood. Nothing really gets accomplished.

So, what's your next step when email isn't working?

Usually, it's a meeting in person or a quick conference call. Unfortunately, those communication methods can create a whole new problem. In an increasingly mobile business world where teams, employees, and customers are spread out over multiple remote offices, work-from-home setups, or field operations, it can be nearly impossible to get everyone into the same place at the same time.

Tethering to the mothership: The lasting value of a virtual phone system

Web conferencing has helped mitigate the above problem. However, the fact that many businesses lack the communication and collaborative tools their team's need — regardless of where they work — is the bigger issue. For example, even with web conferencing, many remote or work-from-home employees still rely on personal cell phones that aren't connected to the company's main phone system.

That's problematic for a couple of key reasons:

- With personal landlines and cell phones, it's significantly more difficult for remote employees to access antiquated company systems for voicemail, call forwarding, and conferencing.
- Without a true company-owned connection between the corporate office and the employee, the relationship between the two feels more like a contract gig than a full-time job — hurting employee engagement and retention.

Thankfully, there's a relatively simple way to solve that problem: implementing a new, company-owned communication system that's flexible, mobile, and collaborative.

One common solution is a VOIP (Voice Over IP) service, which can be based in the cloud or on-site.

The reality is that voice communication is still a far superior — and much more immediate — way for team members to connect with each other. It typically leads to richer, more sincere, and more empathetic communication, which in turn amplifies productivity.

These tools are like a tether to the corporate mothership. They're a lifeline that allows everyone to feel connected to their colleagues and customers, but in a way that aligns with the mobility and functionality that today's remote workers need.

Why many businesses are moving to the cloud

Of course, the image of a desktop phone doesn't exactly convey a sense of mobility. And it certainly doesn't solve the problem of being able to connect from any location.

That's where cloud-based phone systems come in.

Cloud-based phone systems allow team members to receive company calls, access corporate voicemail, and set up virtual conferences from a basic Internet connection.

When employees step out of the office, calls can be forwarded and certain features can be accessed from their cell phone.

Traditional phone systems, on the other hand, often hinder remote workers' communication effectiveness because of their limited mobile capabilities. This often results in lost money, lost productivity, and big headaches. Even worse, businesses often pay more for traditional phone systems in the form of equipment maintenance and outages.

Virtual communication systems create an overall experience that makes people feel like an effective part of the team, wherever they are. No more emotionless email exchanges and no more awkward, disjointed conference calls. At the end of the day, that's good for your team, your company, and, most importantly, your customers.

Battling Bloatware, Trial Programs and Time Bomb Software

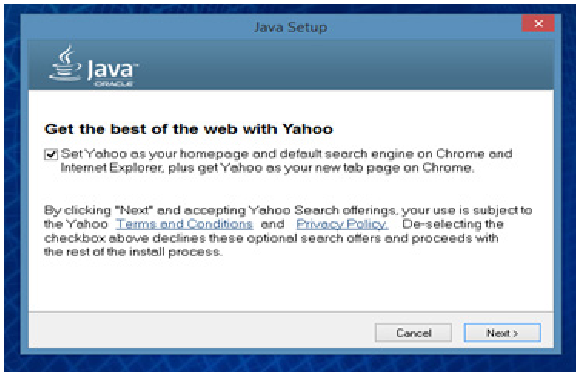
Scott Blake is a Senior Network Engineer with Tech Experts.

The day has finally come. You've saved money for what seems like a lifetime to purchase a new desktop or laptop. You're all excited to get it unboxed and powered on… only to find yourself confronted with loads of bloatware, trial programs and time bomb software you will never use and never asked for. You quickly find yourself spending hours removing all the preinstalled programs instead of enjoying your new device. Why is that?

The sole intent of a vast majority of the programs you find already installed is to track your presence on the web. Some programs, such as Superfish (which Lenovo was installing on their computers), also change your search results so you see different ads than you would from normal browsing habits. This can also affect your computer's security.

Some of the more common programs that tend to get overlooked are browser toolbars. Several of the most common toolbars you will find are Yahoo, AOL, Google and Ask. These are so common that most computer users think they are part of their browser.

The purpose of a browser toolbar is to gather information on your browsing habits such as popular search words or phrases and sites visited. This information is then sold to advertising companies or used to place custom targeted ads on the sites you visit. In most cases, you will also start to see an increase in spam messages in your email inbox. It's recommended to properly remove all browser toolbars from your Internet device.



Get the best of the web with Yahoo

☑ Set Yahoo as your homepage and default search engine on Chrome and Internet Explorer, plus get Yahoo as your new tab page on Chrome.

By clicking "Next" and accepting Yahoo Search offerings, your use is subject to the Yahoo Terms and Conditions and Privacy Policy. De-selecting the checkbox above declines these optional search offers and proceeds with the rest of the install process.

Example of Yahoo piggybacking on a Java install.

Just when you think you have removed everything that needs to be removed, look again. Most likely, you will find trial or time bomb software installed as well. These are programs that offer you their fully functional features for a predetermined amount of time.

Two of the most popular software programs preinstalled in this way are Microsoft Office and anti-virus programs. Office programs will give you full functionality of the Office suite for usually about 30 days, then features will become unavailable to the user after the program expires. In some cases, this has little to no effect on the user, but in other cases, it can have a severe financial impact.

Trial versions of anti-virus programs can be the most devastating to the user. A user will power on their computer, see there is an anti-virus program made by a large and well-known company already installed, and they think they are fully protected against the evils that await them. This may be true for the first 30 to 90 days. However, after the trial period ends, most users either ignore the pop-ups warning that the program is going to expire or they are not notified. This leaves the user in a state of vulnerability. After the program expires, they no longer receive regular security definition updates.

Let's say you have taken the time to fully clean and remove all the bloatware, trial, and time bomb software from your computer. The only things you need to watch for now are third-party programs piggybacking on the installs or updates of other programs.

Two of the most common programs to pay attention to when updating or installing are Adobe Flash Player and Oracle's Java. You need to pay close attention to the installer windows or you will end up spending more time removing unneeded security scanners, toolbars, and/or browsers. For more information about bloatware, trial programs, and time bomb software, contact Tech Experts at (734) 457-5000.

Just when you think you have removed everything that needs to be removed, look again.

Create new service requests, check ticket status and review invoices in our client portal: http://www.TechSupportRequest.com

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

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

Sales Inquiries
(734) 457-5001
(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) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Leasing vs Buying IT Equipment, Which is Better?

When you plan to upgrade or replace computer equipment, there are two ways to do it: Either leasing or buying the necessary IT equipment. As there is no hard and fast rule as to which alternative is better; it heavily depends on your business' unique situation and needs. Here is an overview of each alternative's pros and cons to help you decide between the two options:

When you lease IT equipment, the upfront costs are low, which allows a business to set aside moneys for more pressing needs.

There will be a set monthly payment with no surprises, and your business can keep up with the Joneses when it comes to having the most cutting-edge technology. If some new tech system pops up in a year or two that could help your business operations, upgrading is simple to do when leasing.

There are, however, downsides to leasing. Over the long term, you may pay more for the equipment your business uses. With a lease, there's also the issue of having a contract that usually requires the business to rent the IT equipment for a set length of time.

This means that – even if your business opts to stop using that equipment or it becomes obsolete – the payments still must be made.

When you purchase your business' IT equipment outright, there is only a single, albeit large, hit to the budget, and there's no complicated paperwork to fill out or built-in caveats in the contract to look out for. It belongs to the business and decisions regarding maintenance and method of use are entirely up to those within the company instead of being governed by an outside entity. The purchased equipment can even be deducted from the business' taxes.

On the other hand, putting a lot of money at once into a company's IT needs may draw too much money out of other divisions' budgets, such as marketing, for example. This can negatively impact the business' bottom line. Another consideration is how often technology equipment should be updated. With buying such equipment, it's far harder to upgrade to the latest technologies, which could require waiting for your recently purchased items to sell before making a fresh IT equipment purchase.

Wire Fraud: How An Email Password Can Cost You $100,000

checking the signature before initiating the transfer.

Targeting Employees: Scammers can use a spear phishing attack to install malware on the computer of employees responsible for wire transfers at financial institutions.

From there, the scammer can initiate wire transfers of exorbitant sums to any bank account desired.

The number of ways that scammers can attack financial institutions and victimize individuals and businesses is not limited to these types, either. Scammers will always continue to innovate and develop new ways to take advantage of security flaws.

Spear phishing leads to wire fraud

Spear phishing is a common tactic attackers will use to initiate a wire fraud scheme.

Traditional phishing involves sending an enormous number of emails in hopes of catching a few fish. This approach has grown less effective in recent years due to growing awareness of what the emails look like, so attackers have moved on to a more targeted approach.

Spear phishing involves sending fewer, higher-quality emails to a narrower target. The emails appear to be from a trustworthy source by including personal information or other data acquired by the attacker.

Spear phishing emails are very effective. Their targeted nature gives them a boost in credibility with remarkably better results for attackers.

The emails attempt to lower the individual's guard and often include a malicious link that, when clicked, compromises the individual's machine with a trojan or virus. It can also attempt to get the person to reply with personal information.

Once an attacker receives enough information, he then uses it to attempt wire transfer fraud.