March 2014

TechTidbit.com

brought to you by Tech Experts

Severe Weather Is Just Around The Corner... Be Prepared

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

March is National Severe Weather Preparedness month, and we're still shaking off severe winter storms. Tornado season is right around the corner, so it's important to assess your company's backup systems.

Disasters put all business data at risk and that's why so many businesses take steps to protect their systems. But there are still risks that they may miss.

One of the best ways to make sure your network is properly protected is to learn from the mistakes other companies. Here are four key things that virtually guarantee it will be impossible for your business to recover from a catastrophic hardware failure or natural disaster.

Not backing up data

It may seem like common sense when preparing for a disaster or developing a continuity plan that you should back up your data. However, a study from Symantec found that only half of businesses back up more than 60% of their data.

Other businesses don't back up data or only back up certain systems. This means that if these businesses are faced with a disaster, they could lose up to 40% of their data. Some businesses could lose all of it.

Many experts suggest that businesses not only back up their data, but take more of an all-or-nothing approach. All data should be backed up so that should a disaster happen you can guarantee that nothing will be lost.

Failing to protect off site data

Business is becoming increasingly spread out, with many employees working from outside of the office, or on their own systems. People who telecommute or use their own systems usually store important data on their local machines.

When a company goes to protect or back up their data, some may forget to back up data on machines outside of the company premises.

What's more, some industries have regulations stating that you must back up data from all end-points (e.g., computers and devices) regardless of their location. So, when you are backing up data, be sure that you also back up data on systems that aren't in the office.

Not backing up data consistently

The data in your business is always evolving and growing. Therefore, you need to ensure that it is backed up regularly. Because backups take time, there is a higher chance for them to fail. If you only back up once a year without checking, and disaster strikes, you could find that your data is incomplete, inaccessible or out of date. This may make any recovered data essentially useless.

The question is, how often should you back up your data? For most small businesses, a full backup at least once a week is suggested. If you work with client data on a regular basis or in a regulated industry, daily backups would likely be the best plan.

Using outdated backup methods

Just because you back up your data doesn't mean it will always be available, especially if you use older backup methods such as data tapes or disks. These physical backups can be lost or even destroyed in a disaster and possibly even stolen. You may want to employ a more modern data backup solution that is more reliable, such as our Experts Total Backup cloud backup system.

That being said, you don't have to give up older methods as these can come in handy, especially if you are going to be operating without the Internet for an extended period of time. By employing more than one solution, you can cover all bases while ensuring that data is largely backed up and available.

If you are looking to learn more about how you can protect your data, please contact us today to see how our systems and solutions can help.

Tips For Defending Against Soci

by Michael Menor,
Network Technician

I just got yet another email from my bank. Or, at least it looked like the bank that had issued one of my credit cards. The email included my correct name and mailing address, as well as a variety of other quality information such as the last four digits of my credit card number.

This may not seem like it is great information, but I regularly change details in my name for accounts, such as using different middle initials, including or omitting part of my first name, or using one of the three different street addresses that will get mail delivered to my home. So when someone gets it all correct, it really is a big deal to me.

According to the email, I needed to log on (yes, convenient link included) and check a fraud alert that was being issued on my credit card by my bank because of suspicious activity.

Again, this did make some sense, because this account was compromised, and I do have fraud triggers set to alert via email and text. Despite the fact that I pretty much always view these emails as suspicious, all in all, it seemed like the type of email that I might not want to ignore.

Except for the fact that the email came to a valid email address which I have never registered with this particular bank. Oddly enough, I have seen this with increasing frequency, and have received both Facebook and LinkedIn notifications with friend/connect requests - with people I actually know - but, both sent to email addresses which I have never registered with Facebook or LinkedIn.

Social Engineering?

Getting a few emails doesn't necessarily mean I am in the middle of a social engineering attack. The catch here is that the emails contained real information that could only be gathered if someone was working it, so I tend to look a little beyond random phishing. The sender had good information.

A more recent complexity in social engineering is the use of this type of good information in an Advanced Persistent Threat (APT). In this role, social engineering is used in concert with other attack vectors. Information gathered from social engineering is used to target technical attacks, and in turn, information from technical attacks is used to help target further social engineering attacks as an attacker learns more about a set of individuals as well as the entire organization.

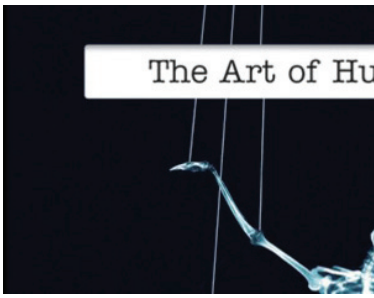
The availability of information from public sources like social media allows online research about specific people to be very targeted, further enabling more specific social engineering attacks.

Part of the social engineering attacks that are the most dangerous are those attacks that also try to get targets to execute malicious links or applications, potentially installing malware.

You may recognize a random external email attack that includes a virus or a malicious link. But, how would you respond to an email from your daughter's college that appears to claim she was being ejected, or an email from a well-known pharmaceutical company that announced recently discovered potentially fatal side effects of a prescription drug that you are currently taking? Personal attacks like this which are tailored to a specific individual have become more common, and we should expect this trend to continue.

Can We do Anything About It?

Since there is no such thing as a personal firewall to help filter out attacks, the single best thing you can do to minimize the chances of a successful social engineering attack is proper awareness. At the same time, some technical controls can help. I have no "magic list" of five things to do, and I know 16 controls can look like a daunting task, but any or all of these things can help reduce the chances of a successful social engineering/phishing attack.



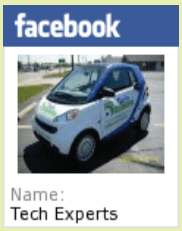
Even starting with one thing that you are currently not doing can help.

1. You should know that social engineering attacks exist. You should also know that attackers are interested in getting personal information as well as corporate information, and that individuals may be attacked through any phone, email or social media account - both work and personal - since personal knowledge can help make targeted attacks more successful.

2. You should be very careful about the type of information you leave in your voicemail greeting. A good default is to leave your first name, and state that you will return the call, without identifying your group.

3. "Extended absence" messages may be necessary, but should be used with care. Consider leaving a "fake" alternate contact name so that a coworker can easily identify that the call came from your out-of-office message. When you're out and you want callers to reach "Betty Brown" for assistance in your absence, you might leave an outgoing message that says "Beth Brown" instead of "Betty Brown." Then, when a caller asks for "Beth," Betty will actually know that this call came as a result of your out-of-office message.

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

ial Engineering Attacks

4. To help minimize the ease with which an attacker can identify valid email addresses at your organization, your email server should be configured so that it does not respond to inbound invalid addresses.

5. Make sure that corporate email addresses have little to no relationship with the employee's user ID. Never make the name in your email address the same as the user ID you use on your internal network. If the user ID that you use to log onto your corporate network is bsmith, do not make your corporate email address bsmith(at)yourcompany.com.

6. You should be filtering attachments on your email and removing attachments with potentially hostile contents, such as executable files. Distributing Trojan horses or viruses via email is a common attack technique.

7. Be aware of company specific jargon. Anyone who uses improper or general information about your company can be regarded as an outsider. Maybe you work for Tech Experts, but everyone calls it "TE." Using incorrect terminology is a clue that a call may not be genuine.

8. Someone who acts irate or angry and attempts to rush you through a questionable process should be regarded as suspicious. Bullying someone is a common technique to keep a target off balance.

9. Many (not all) data gathering emails come from temporary or "throw away" accounts, such as an account at Gmail or Yahoo. Your staff should be aware that there are a number of reasons an attacker would like to clearly identify valid email addresses and that your staff should consider this in all external responses.

10. Your company should not use or allow the use of external web-based email accounts through the normal course of your business. Do not let employees get used to seeing official email from such accounts (like @gmail.com instead of @yourcompany.com).

11. Your employees should know that no one from corporate IT (or anyone else) would ever call them and ask for their password. Simply put, no employee should ever divulge his or her password to anyone else. Never.

12. You should maintain an accurate and current employee directory with phone numbers. Anyone receiving a suspicious call can ask the caller who they are and consult the phone directory for the name and phone number.

13. Dispose of sensitive material in an appropriate manner. Either use an office shredder or contract with a reputable "secure disposal" company to dispose of sensitive information for you. Yes, "dumpster diving" is real, does happen and does work.

14. The Help Desk can take steps to reduce the number of invalid password resets and snooping attempts.

a. If a user calls from an outside number, the Help Desk's first response should always be to consult a corporate phone directory for an official work, mobile or home phone number to return the user's call. Any number not on the list should be considered suspicious.

b. The Help Desk should verify the employee's full name, with proper spelling, phone extension, department or group. You are trying to add enough information that an attacker would have to be very prepared for the request.

c. The Help Desk should ask the caller for a number at which they can call the user back, regardless of from where the user is calling. A call from anyone who will not provide a callback number should be considered an attack.

d. You may consider having the Help Desk leave a user's new password in the employee's corporate voicemail. A valid user should have no trouble retrieving the password. An attacker would have to compromise the voicemail system to get access to the password.

15. If you are being asked to release or reveal something that is clearly sensitive, such as your strategic plan, passwords, pre-release earnings, source code and other such internal information, it should be automatically regarded as suspicious.

16. You should have a plan for how you will communicate internally if you identify that a social engineering attack is taking place against your company.

Does every employee get an email stating that an attack is in progress, and that everyone should exercise additional care? Who should send the email, and what is the final triggering event before a company-wide alert is distributed?

Conclusion

A good social engineer can extract sensitive internal information very quickly, and can then help ensure they make the best use of that information to further additional attacks.

Knowing this, you should understand that a social engineering attack can happen at any time. They don't happen because you have poor security, they happen because someone else decided you were a target.

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

Browser Wars: Which Browser Should You Use?

by Lino Perna, Technician

Since its public release in 2008, Google Chrome has been taking its place in people's hearts and minds, replacing the commonly used Internet Explorer.

Ever since then, these two browsers have been at constant war. The public loved the fresh, simplistic, elegance of Chrome which left Internet Explorer in its dust.

Now, after all these updates and changes, which of the two has made the most positive progress? Which browser is better?

Internet Explorer

Internet Explorer was the most widely used browser up until 2008. It had the internet navigation world in the palm of its hands, and because of its massive success Microsoft decided not to change anything.

Internet Explorer came standard with every new Microsoft computer, so to the general public, that was the only option. Yes there were other web navigators, but this was the best.

In its current state, Internet Explorer 11 is faster and more efficient than any other previous versions. The security and privacy features are phenomenal and coveted by other browsers.

In a general sense, the interface is usable, but may be too complicated for some users. While it doesn't have site prediction or voice search, it is still faster and better than ever for everyday tasks.

Chrome

When Chrome was first released, it had low usage percentage because it was an unknown browser, but at that point, Firefox had become prominent and had passed up Internet Explorer.

Slowly but surely, Chrome became more widely known and used. It took until 2011, but finally overcame the competition and became the most used browser in the world.

Today, Chrome reigns over the other browsers. Its usage surpasses any of the other browsers, but the question is: Why? The reasoning for the era of Chrome is its design.

It's easy enough for an individual of any age to use. It simultaneously possesses the ability to give you luxuries such as: a drop-down box with thumbnails to easily access your favorite websites or the integration of Gmail and Youtube.

The simplicity of it contributes to the unparalleled speed that it possesses. Speed, efficiency and quality are the necessary staples of success.

Google Chrome possesses all three of these essential attributes that helped it achieve and sustain dominance over its predecessors.

The built in flash player and PDF support put Chrome ahead of the competition because both tools are used quite frequently in both a business and scholastic setting.

Wrapping Up

It all comes down to this: When it comes to efficiency, speed, and quality, Chrome takes the cake.

Its facile interface, outstanding quality, and unmatched speed rocket it past Internet Explorer, and any other browser at that.

Though Internet Explorer may be easier to access, if you want a browser that can do all you ever needed and more, while also being considerably faster than its competition, Google Chrome is the browser for you.

Tech Tips For The Road Warrior

Traveling is rarely guaranteed to go smoothly, but there are at least a few travel headaches that can be kept at bay thanks to technology. If you know how to make use of it in the proper manner, technology can increase your likelihood of having a positive experience on your next vacation.

One good tip is to use tech to keep updated on your flight status. Flights are commonly disrupted due to one reason and another, and delays and cancellations et al can be tough to keep up with. Many airlines today however enable you to track your flight status via a website or app, so if you own a smartphone you can stay updated on what is happening with your flight no matter where you are. If an app is offered by your airline for this purpose, be sure to download it and ensure your smartphone has been fully charged before you set off to the airport.

Translation apps are another good idea if you are jetting off to foreign climes. Many translation apps on tablets and smartphones are free of charge, and also have voice recognition software, meaning that communicating with people who speak a different language has never been easier.