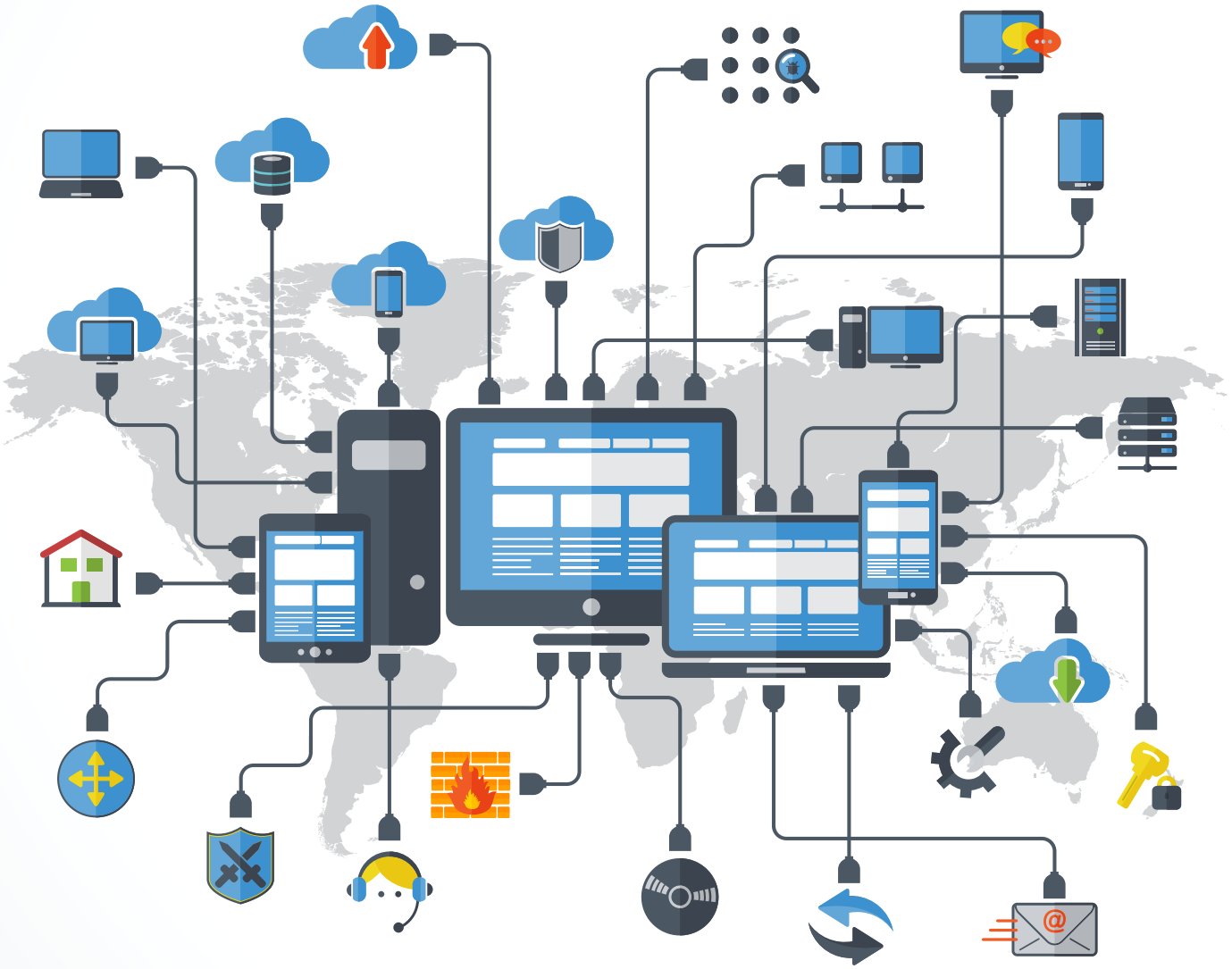
Cybersecurity Business Training

An Employee's Guide to Preventing Business Cybercrime



ANDERSON TECHNOLOGIES

A Handbook by Anderson Technologies, a St. Louis IT Company
info@andersontech.com | http://andersontech.com | 314.394.3001

Cybercrime Is on the Rise

Cybercrime is the fastest-growing threat to businesses and individuals in the United States. Perpetrators use nefarious tactics and tools like Trojan horse viruses, spyware, bots, phishing, and spear phishing to perform a host of crimes, including fraud and theft of valuable data like credit card numbers, passwords, and personal health information.

In 2015, more than half a billion personal records were lost or stolen, and that figure may be even larger because cybercrime often goes unreported.[1]

Most cybercrime is preventable, but even if you are doing everything right, it takes just one wrong click to breach your digital "fortress." That's why it is so important that all members of a business team understand digital best practices and how to protect themselves from cybercrime.

In this handbook, you will learn about:

- The state of small business cybercrime
- Email red flags, including examples of real spear phishing emails
- Internet safety tips and warning signs
- What to do if you've clicked or downloaded something you shouldn't have

Cyber Threats Against Small Businesses Are Growing

Over the last few years, cybercriminals have started targeting small businesses more frequently. According to Symantec,[2] 43 percent of all spear phishing attacks were against small businesses with fewer than 250 employees. A survey by the U.S. National Small Business Association showed that the average hit to a hacked small business's bank account was $32,000.[3]

Part of the reason small businesses are increasingly targeted is because many do not take the necessary steps to stay secure. That makes them easy targets.

To ensure their digital safety, every small business must:

1. Install a hardware firewall that is continuously monitored and patched.

2. Install anti-virus and anti-malware software on all devices and keep them updated.

3. Back up all business-critical files regularly and test their ability to be restored.

4. Regularly update all devices with the latest operating system and third-party application patches.

5. Adopt a password policy appropriate for your business.

6. Educate employees about safe digital practices.

That last one is important. Even if you are completing steps one through five diligently, it only takes a single bad decision by one employee to throw all your hard work out the window.

Cybercriminals Are More Sophisticated

Phishing emails are a cybercrime tactic in which the sender tries to illicit personal information from the recipient. They are sent to a wide audience and are often recognizable as fraudulent because of the nature of the content, strange spelling errors, or unnatural syntax. For example, you may have received an email from a "prince" in some faraway country who is eager to give you millions. Most employees are aware that such emails are hoaxes.

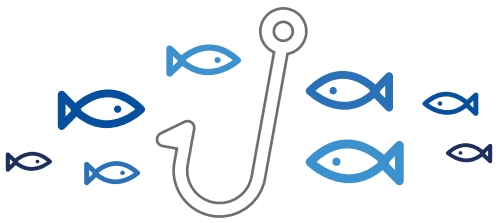
Unfortunately, the bad guys have gotten better. Phishing has evolved into spear phishing, a similar but more sophisticated con in which a criminal targets a specific person and crafts a believable email based on personal information obtained about the recipient.

Spear phishing emails often appear to come from a colleague, friend, family member, or business associate. They are usually well-designed and written convincingly enough to seem completely legitimate.

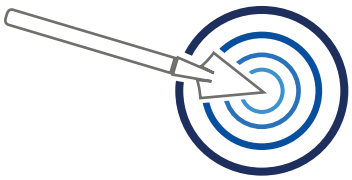
How Do Hackers Get My Info?

Even if you've done everything right, cybercriminals could still glean enough information to target you via a phishing scam. For example, they may have hacked a site that has your contact information, such as an online shopping company or an email provider. In December 2016, Yahoo confirmed more than 1 billion user accounts were compromised in a security breach.[4] This is the type of incident that can give cybercriminals the information they need for more convincing scams.

Hackers also target you by researching information you willingly share on the web, such as posts on social media sites or your contact information.



Phishing: These emails go out to a wide audience in hopes someone will fall for the scam.



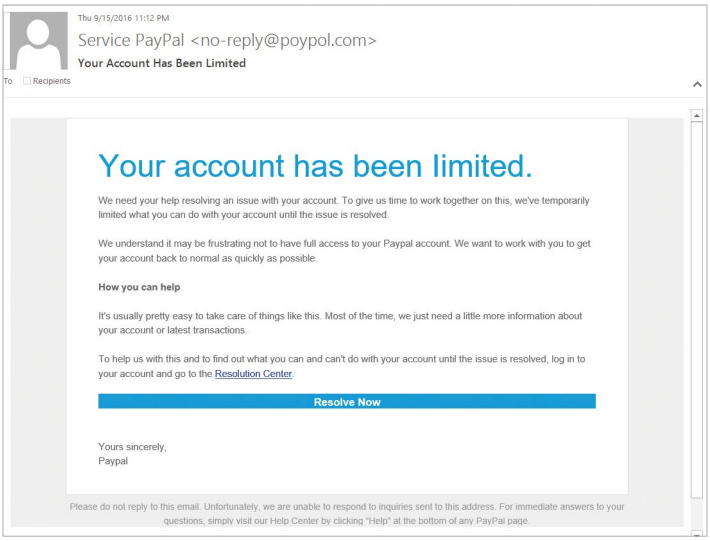
Spear Phishing: These emails are personalized and designed to trick a particular target. They are harder to recognize as fraudulent.

Your Email Best Practice Checklist ☑

The screenshots below show actual examples of spear phishing emails. As you can see, they look quite convincing. Fortunately, the act of opening an email doesn't usually do any harm. It's clicking a subsequent link or downloading an attachment that allows the criminal to infiltrate your system.

Actual Examples of Spear Phishing Emails

Example A

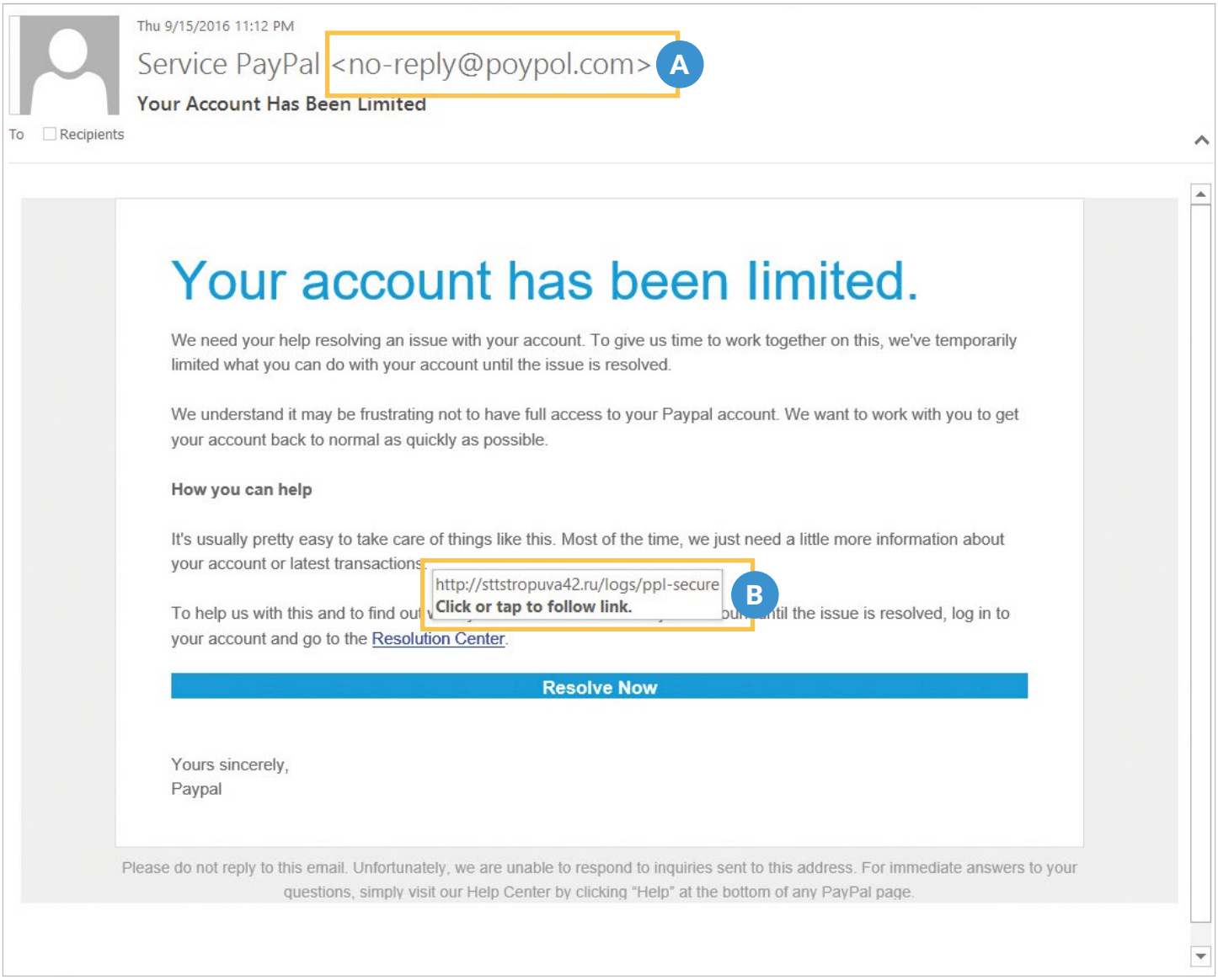


Example B

Your Email Best Practice Checklist ☑

Although spear phishing emails can be convincing, there are ways to identify them as fraudulent before you click a dangerous link.

Example A



A Incorrect Email Address

Examine the email address. Notice that in this example, the email address uses "poypol.com" instead of "paypal.com."

B Suspicious URL

Hover your mouse over a link before clicking. Notice that although this URL includes the word "secure," it is actually leading to a website in Russia, as indicated by the .ru extension.

Your Email Best Practice Checklist ☑

Here's what you need to think about every time a new email hits your inbox.

1. Are they asking me for private or personal information?

Consider the nature of what the sender is asking for. Financial organizations will NEVER ask you to provide personal information like account numbers or passwords via email. Email, by its nature, is not secure. A legitimate bank will only ask for private information via a secure site after you have already proven your identity, ideally by a two-factor identification process (in which you take two steps to prove you are who you say you are, such as entering a password and answering a security question). Go on immediate alert if a sender is asking directly for personal information.

2. Does it seem too good to be true?

Phishing emails are sometimes recognizable because they are promising something that seems too good to be true. Spear phishing emails are more subtle and realistic than phishing emails, so always be on high alert, remain skeptical, and remember, if something seems too good to be true, it probably is.

3. Where does this link lead?

Before clicking on a link, hover over it with your mouse to see the URL. This can be a tip-off. If the URL does not match the sender's supposed company, be wary. Also be wary of URLs that end in domain names from foreign countries, like on the previous page in which the URL posing as a PayPal site actually directed to a website in Russia.

4. What is the email address of the recipient?

Check the actual email address of the sender, not just the name that shows up during your Inbox preview. Does the sender have a Yahoo address even though they claim to be with a business? Are there spelling errors, like the one in the "no-reply@poypol.com" example?

5. Are there attachments?

Attachments are a huge red flag! By downloading an attachment, you could infect your computer, or even your entire business network, with malware or viruses. Do not download an attachment unless you are certain of the sender's identity and the content seems legitimate. If you weren't expecting to receive an attachment from the sender, even if you recognize him or her, consider contacting them to confirm that they've sent it. If you do download an attachment, save and scan it with anti-virus software before opening it.

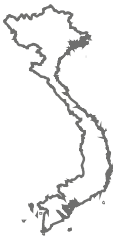
Country Domain Extensions Known to Be Cybercrime Hotspots

Russia - .ru

China - .cn

Brazil - .br

Vietnam - .vn



Nigeria - .ng

The Rules for Safe Surfing

Employees also need to be mindful of web-browsing best practices. With one wrong click, you could infect your computer with dangerous malware that allows a criminal to affect your computer's performance or obtain personal information about you, your business, or customers. You cannot passively surf the web. Be alert, think before you click, and try not to visit sites you've never heard of. Here's what you need to know.

1. Seedy content breeds seedy behavior

Cybercrime is rampant on sites where people are doing something they probably shouldn't be. Pornography and anything illegal are prime targets for cybercriminals, in part because the sites' administrators probably aren't taking the steps necessary to protect their visitors. Stay off these types of sites—especially at work or when you are remotely connected to your work network.

2. Dangerous sites can show up in searches

Even innocuous behavior can land you in dangerous territory. Criminals can create sites cleverly designed to trick users into believing they are legitimate. Plus, "real" sites can get hacked. Let's say you are searching for a gift on your lunch break and end up on a small e-retailer you have never heard of, a site that happens to have been hacked. A criminal could access your password and credit card information when you enter it on the affected site!

3. Use the "safe search" feature

Anti-virus and anti-malware programs often offer a "safe search" feature in which they'll run search results through their own database to rate the safety of sites and flag any URL they know to be compromised. If your business takes this security precaution, do not visit sites that aren't deemed safe by your anti-virus provider.

4. Install a firewall for enhanced protection

A firewall is a virtual fence between your network and the outside world and is designed to keep an attacker from accessing your network from an open port or protocol. An enterprise-level firewall can include additional features that enable businesses to filter out certain types of content and add additional layers of malware protection. If you don't have a firewall, a managed services provider can help you set one up and provide the necessary ongoing maintenance of firewall settings. But remember, firewalls can't block everything, especially not zero-day threats, new viruses that are written to take advantage of previously undocumented flaws in a piece of software. Always stay alert and follow cybersecurity best practices.

(Continued on Next Page)

The Rules for Safe Surfing

(Continued from Previous Page)

5. Be careful about downloading things from the web

Cybercriminals can do their damage by getting you to click a web link or download a nefarious attachment. The absolute safest approach would be to never download anything from the web, but we know in today's business environment, that is not realistic. Proceed with caution, always scan files before downloading them, and if you are unsure if something is safe, run it by your IT partner or your boss first.

6. Exercise caution when working remotely

It's increasingly common for employees to work remotely, whether from home, a public place, or on the road as part of business travel. While this is certainly convenient, it poses major cybersecurity risks. Whenever you are utilizing a company asset (such as a laptop computer, tablet, or smartphone), think before you connect to a Wi-Fi network. Even your at-home connection could be dangerous! If your home environment is not fully protected with up-to-date operating system patches, anti-virus definitions, firewall firmware, etc., it could be laced with problems. If you connect your company laptop, you could infect it and bring the virus back to your workplace.

How to Tell If an Online Retailer Is Legitimate

1. Check for a SSL Certification by seeing if the URL starts with HTTPS instead of HTTP. "S" stands for "secure" and means that the site has gone through a validation process.

2. Make sure the site name looks legitimate, doesn't have strange spelling errors, and isn't trying to imitate a well-known site.

3. Confirm the site has a physical address and phone number.

4. Check for a privacy policy, return policy, and other signs that the site is legitimate, such as a social media presence and user reviews.

5. Use common sense! If something seems too good to be true (i.e. the prices are incredibly low) be skeptical and leave the site.

So What Can the Bad Guys Really Do to Me Anyway?

There are a host of ways criminals can threaten your personal security and your business. They can steal personal information, steal business data, infiltrate your network so they can access other people's data, and even render your entire computer or network unusable. In ransomware attacks, perpetrators freeze a person's computer or network until they agree to pay a monetary sum. Ransomware attacks against small businesses are on the rise, so it is important your business takes precautions.

The Art of Password Management

In 2015, the two most common computer passwords were "123456" and "password."[5] This is unacceptable! Cybercriminals use software that help them crack passwords, and with such weak passwords, they don't even need assistance. Take the following steps to improve password security.

1.
Do not use the same password for everything.

2.
Use complicated passwords with a combination of uppercase and lowercase letters, numbers, and symbols. Avoid obvious things like names of loved ones or birthdates.

3.
Don't use a password that is a real word that could be found in the dictionary.

4.
Use a minimum of eight characters. Longer passwords are even stronger.

5.
Change your passwords frequently.

6.
Consider a password management tool to help you keep track of passwords.

7.
If you ever fear your cybersecurity has been compromised, change your passwords immediately.

"Uh-oh!"

What to Do When You Think Cybersecurity Has Been Compromised

Following digital best practices will help you avoid cyber threats, but the bad guys are so sneaky that they can trip up even the most cautious among us. Mistakes happen.

Sometimes a virus will go completely unnoticed. Other times, it may affect computer performance, especially if you have an older machine.

If you click a link and don't feel comfortable with where it leads or what pops up, download an attachment and are apprehensive about what happens next, or simply feel unsure for any reason, trust your instincts and take the following steps.

- Don't click anything, not even an "X" to close a pop-up box.
- Disconnect from the network by either physically removing the network cable if your machine is hardwired or by turning off your computer's Wi-Fi connection.
- Reboot your computer in Safe Mode and run a full system scan with your anti-virus and anti-malware software.
- If an unresolved issue is identified, ensure you have an existing backup of your data, reformat your hard drive, reinstall the operating system, reinstall all third-party software, and restore your data from the known good backup.
- Perform a second system scan to ensure your machine is clean.
- Update all critical passwords. Monitor your sensitive data and financial accounts.
- Call your IT partner at any time if you need assistance.

If you didn't actually click the harmful link or download anything dangerous, a simple reboot may be all you need. If everything appears fine, ensure your anti-virus and anti-malware software is up-to-date and run a full system scan. Clear your browser cache (a good step to take routinely anyway) and change your passwords for extra security.

"X" Does Not Mark The Spot

If you are suspicious of a pop-up, don't try to close the window by clicking the "X"! Even though you are trying to dismiss the threat, the simple act of clicking could be enough to infect your computer. Instead, disconnect from your business network and call an IT expert right away.

The Bottom Line? Be Skeptical.

Be skeptical about every email you receive and every website you visit. **Do not move passively through the digital realm.** Liken it to a bustling foreign bazaar with a notoriously high rate of theft. You wouldn't move through this shopping center giving out information to every random person who asked. **Stay alert and think before you click.**

Endnotes

[1] Symantec, "2016 Internet Security Threat Report," Vol. 21, symantec.com, date posted April 2016, 6. https://www.symantec.com/security-center/threat-report.

[2] Ibid., 43.

[3] National Small Business Association, "2015 Year-end Economic Report," nsba.biz, date posted Feb. 9, 2016, 12. http://nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.

[4] Vindu Goel and Nicole Perlroth, "Yahoo Says 1 Billion User Accounts Were Hacked," *New York Times*, Dec. 14, 2016. http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

[5] Morgan, "Worst Passwords of 2015," TeamsID, date accessed Dec. 19, 2016. https://www.teamsid.com/worst-passwords-2015.

About Anderson Technologies

We hope you found this handbook useful. Educating yourself and your team is an integral and often overlooked component of cybersecurity.

Anderson Technologies is a St. Louis company that optimizes technology to meet the demands of small businesses. Anderson Technologies' team of experts specialize in small business cybersecurity and help businesses take the steps necessary to ensure optimal digital health. Whether frustrated by hassles and glitches or looking for a trusted partner to provide small business IT support and configure your systems for growth, Anderson Technologies can help.

Click to Schedule a Free Consultation

Have Any Questions?

The team at Anderson Technologies is happy to discuss any questions you might have or schedule a time to help you educate your employees about best practices. Give us a call today at 314.394.3001.

ANDERSON TECHNOLOGIES