Cybersecurity

Guidelines for Secure Behavior Online and in the Office

THRIVEON
INFORMATION & TECHNOLOGY

Contents

E-Book
Cybersecurity
Guidelines for Secure Behavior
Online and in the Office

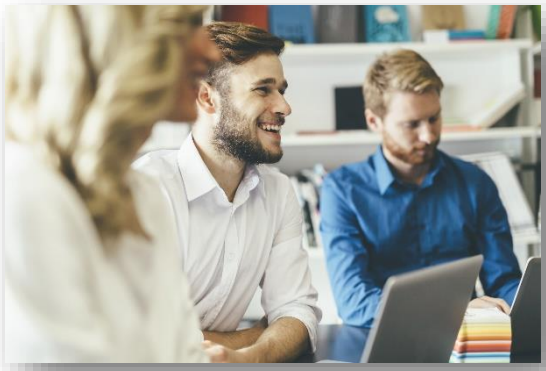
Introduction

The Need to Educate Employees on Cybersecurity

When developing cybersecurity programs, many businesses focus on protecting their infrastructure perimeter and device endpoints. After all, that's where cybercriminals usually first gain access and wreak havoc on a company's digital access.

But it's also important to consider what happens when a threat bypasses perimeter defenses and targets an employee – in the form of a malicious email or text, or even a voicemail that might prompt an employee to respond with confidential company information. There's also the possibility of an offline attack from inside the office, where an employee or an office visitor might gain access to valuable data by quickly taking something carelessly left on a desk.

According to a PricewaterhouseCoopers survey, in 2014, 69% of business executives expressed concern about cyber threats, including a lack of data security. In 2015, an updated survey increased that number to 86%. These numbers indicate that it's clear there's a pressing need for better cybersecurity. The issue is not going away anytime soon. If anything, it's only getting worse.



Stronger cybersecurity has become a global priority over the last few years as hackers penetrate the IT infrastructure of government and enterprises with increasing frequency and sophistication. According to a study conducted by the Identity Theft Resources Center, the total number of data breaches reported in the US grew from approximately 400 in 2011 to approximately 750 in 2015. This represents an increase of more than 60% and does not include breaches that went unreported – a figure that is likely higher.[1] Coupled with the Internet of Things (IoT) and the explosive growth of mobile devices, the threat landscape and potential for data leaks is even more significant.

1. Business Insider, "This one chart explains why cybersecurity is so important," 4/5/2016: www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-31

The importance of security awareness for your employees

In this E-Book, we explore the need for employees to practice strict and secure cybersecurity habits – not only to thwart digital attacks, but also to prevent someone from simply walking by their desk (in the office or at home) and picking up a device or document that contains sensitive information. We also present the key steps SMB business owners and executives can take to educate their employees to help secure their company's data and intellectual property.

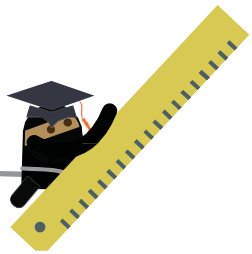
We can't stress enough the importance of security awareness training for internal employees. Education them on what it takes to protect proprietary documents and data is critical. Any leaks – unintentional and intentional – could hurt the business in the form of information that assists a competitor, violates regulations, or harms the corporate image. Leaks can also hurt employees from the standpoint of personal information that might be exposed.

Lastly, customers and business partners could be at risk, compromising the industry reputation of any business that does not properly protect confidential information. It only takes one incident to completely destroy any goodwill you established and built with your customer base.

Do you invest in or recognize the need for cybersecurity?

82 percent of SMBs say they're not targets for attacks as they don't have anything worth stealing (Towergate Insurance).

In a Webroot survey, less than a quarter of respondents indicated having a dedicated in-house cybersecurity team or individual (Webroot 2015 SMB Threat Report).



Chapter 1

Physical Security Precautions

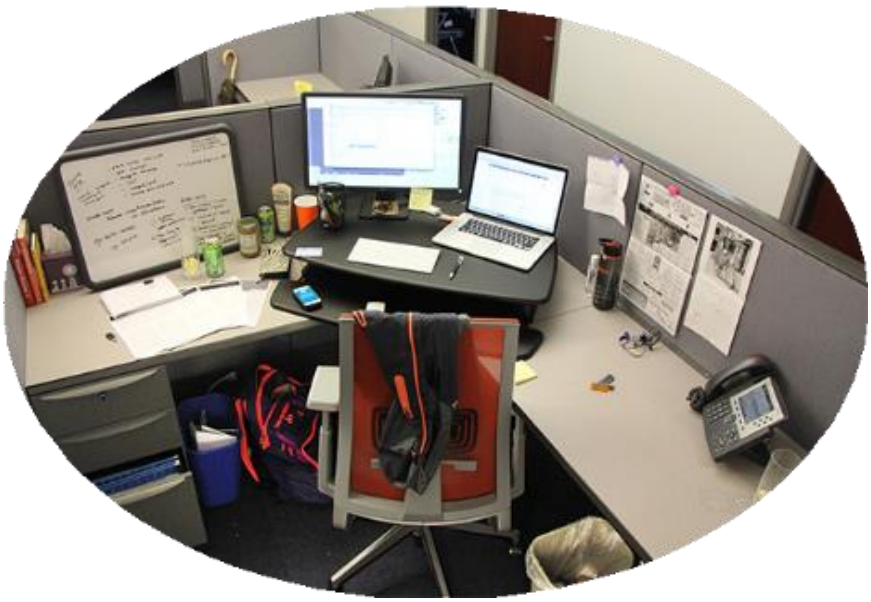
Start the Cybersecurity Discussion with a Clean Desk

It makes complete sense and sounds so simple, but keeping a clean desk is often overlooked when talking about data security. It's also the perfect place to start the discussion with employees.

Employees that keep a cluttered desk tend to leave USB drives and smartphones out in the open. They also often forget to physically secure their desktops and laptops so someone can't somply walk off with them.

A messy desk also makes it more difficult to realize something is missing such as a folder with hard copy print-outs of customer lists. In addition to increasing the likelihood of something being removed, a cluttered desk means that the discovery of any theft will likely be delayed—perhaps by days or even weeks if the employee is out of the office. Such delays make it more difficult to determine who the perpetrator is and where the stolen material might now be located.

Encouraging employees to maintain a neat desk pays off in two ways. In addition to making digital and paper assets more secure, employees with clean desks are more apt to be productive because they can quickly—and safely—access the tools and resources they need to do their jobs.



What's wrong with this desk?

The Common Messy Desk Mistakes to Avoid

The following list presents 11 "messy desk" mistakes employees are prone to commit and which could cause irreparable harm to the business, the employee, fellow employees, customers and business partners. These are all bad habits for which to educate employees to stop:

1. Leaving computer screens on without password protection: Anyone passing by has easy access to all the information on the device; be sure to lock down screen settings.
2. Placing documents on the desk that could contain sensitive information: It's best to keep them locked up in drawers and file cabinets.
3. Forgetting to shred documents before they go into the trash or recycling bin: Any document may contain sensitive information; it's best to shred everything rather than taking a risk.
4. Failing to close file cabinets: This makes it easy for someone to steal sensitive information and more difficult to realize a theft has occurred.
5. Setting mobile phones and USB drives out in the open: They likely contain sensitive business or personal information and are easy to pick up quickly without being caught in the act.
6. Neglecting to erase notes on whiteboards: They often display confidential information on products, new ideas and proprietary business processes.
7. Dropping backpacks out in the open: There's often at least one device or folder with sensitive information inside.
8. Writing user names and passwords on slips of paper or post-its: This is especially important given that user names and passwords are typically used to log in to more than one site.
9. Leaving behind a key to a locked drawer: This makes it easy to come back later—perhaps after hours when no one is around—and access confidential files.
10. Displaying calendars in the open or on the screen for all to see: Calendars often contain sensitive dates and/or information about customers, prospects and/or new products.
11. Leaving wallets and credit cards out on the desk: This is more likely to impact the employee, but wallets may also possess corporate credit cards and security badges.

In today's fast-paced world where employees are always on the go, it takes too much time to determine whether documents, USB drives, devices and other items contain sensitive information. The safe bet is to make sure everything is filed away and kept locked up or else properly destroyed.

Chapter 2
Email Threats

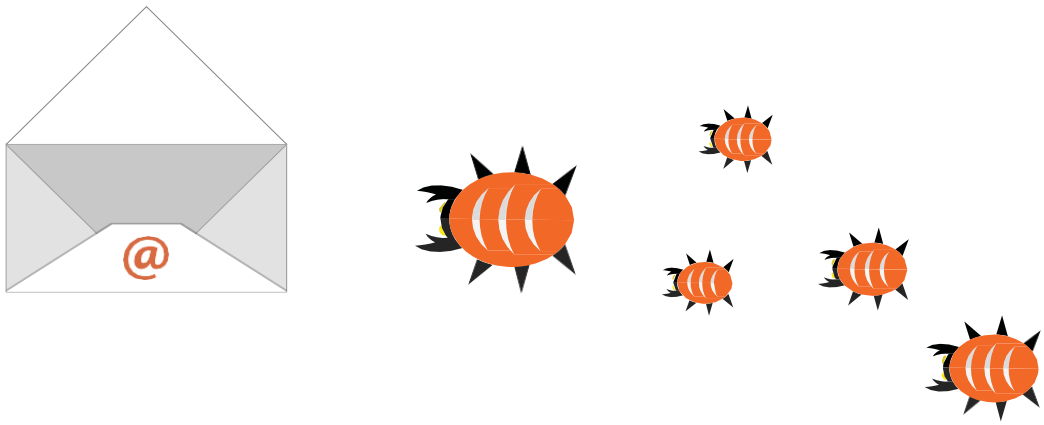
Social Engineering Inboxes and VoiceMail

Social engineering is non-technical, malicious activity that exploits human interactions to obtain information about internal processes, configuration and technical security policies in order to gain access to secure devices and networks. Such attacks are typically carried out when cybercriminals pose as credible, trusted authorities to convince their targets to grant access to sensitive data and high-security locations or networks.

An example of social engineering is a phone call or email where an employee receives a message that their computer is sending bad traffic to the Internet. To fix this issue, end users are asked to call or email a tech support hotline and prompted to give information that could very likely give the cybercriminal access to the company's network.

Phishing Email Compromises

One of the most common forms of social engineering is email phishing—an attempt to acquire sensitive information such as usernames, passwords and credit card data by masquerading as a trustworthy entity. Phishing is likely the #1 primary email threat employees need to focus on.



2. RSA Conference, "How a Security CEO Fell Prey to Scammers (Almost)," 3/3/2016: http://www.rsaconference.com/blogs/security-ceo-scammers#sthash.egMiB2xW.dpuf2

Such emails often spoof the company CEO, a customer or a business partner and do so in a sophisticated, subtle way so that the victim thinks they are responding to a legitimate request. The FBI says CEO (or C-level) fraud has increased 270 percent in the past two years with over 12,000 reported incidents totaling over $2 billion dollars in corporate losses.[2]

Among the reasons these scams succeed are the appearance of authority—staffers are used to carrying out CEO instructions quickly. That's why phishing can be so easy to fall victim to.

Four Common Phishing Techniques

The scope of phishing attacks is constantly expanding, but frequent attackers tend to utilize one of these four tactics:

1. Embedding links into emails that redirect users to an unsecured website requesting sensitive information.
2. Installing Trojans via a malicious email attachment or posing ads on a website that allow intruders to exploit loopholes and obtain sensitive information.
3. Spoofing the sender address in an email to appear as a reputable source and requesting sensitive information.
4. Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

Email Security Best Practices: 5 Ways to Block Phishing Attacks

Employees should always be suspicious of potential phishing attacks, especially if they don't know the sender. Here are five best practices to follow to help make sure employees don't become helpless victims:

1. Don't reveal personal or financial information in an email—Make sure employees also know not to respond to email solicitations for this information. This includes clicking on links sent in such emails.

2. Check the security of websites—This is a key precaution to take before sending sensitive information over the Internet. <http> indicates the site has not applied any security measures while <https> means it has. Also consider if employees are practicing safe browsing habits.Sites that do not serve a legitimate business purpose are also more likely to contain harmful links.

3. Pay attention to website URLs—Not all emails or email links seem like phishing attacks, so employees may be lured into a false sense of security. Teach them that many malicious websites fool end users by mimicking legitimate websites. One way to sniff this out is to look at the URL (if it's not hidden behind non-descript text) to see if it looks legit. Employees may also be able to detect and evade the scheme by finding variations in spellings or a different domain (e.g.,.com versus .net).

4. Verify suspicious email requests—Contact the company they're believed to be from directly. If an employee receives an email that looks odd from a well-known company, such as a bank, instruct them to reach out to the bank using means other than responding to the suspicious email address. It's best to contact the company using information provided on an account statement—NOT the information provided in the email.

5. Keep a clean machine—Utilizing the latest operating system, software and Web browser as well as antivirus and malware protection are the best defenses against viruses, malware and other online threats. It may be difficult for employees to do this, so the business may want to invest in a managed IT services provider who can also be a trusted advisor for all IT needs.

Chapter 3
Username and Password Management

Low Security Account Credentials

Although it should be common sense, employees need to avoid the use of passwords that are easy for hackers to guess. Among the top ten worst passwords according to www.splashdata.com are those that use a series of numbers in numerical order, such as <123456>. The names of popular sports such as <football> and <baseball> are also on the list as are quirky passwords such as <qwerty> and even the word <password> itself.

Emphasis should also be placed on the importance of avoiding common usernames. In analysis conducted by the information security firm Rapid7, hackers most often prey upon these 10 usernames in particular[3]:

- Username
- Administrator
- Administrator
- Admin
- User1
- Alex
- Pos
- Demo
- Db2admin
- sql

Lifehacker, "The Top 10 Usernames and Passwords Hackers Try to Get into Remote Computers," 3/3/2016: http://lifehacker.com/the-top-10-usernames-and-passwords-hackers-try-to- get-i-17626382433

How Attackers Exploit Weak Passwords to Obtain Access

While most websites don't store actual username passwords, they do store a password hash for each username. A password hash is a form of encryption, but cybercriminals can sometimes use the password hash to reverse engineer the password. When passwords are weak, it's easier to break the password hash.

Here is a list of common word mutations hackers use to identify passwords if they feel they already have a general idea of what the password might be[4]

- Capitalizing the first letter of a word
- Checking all combinations of upper/lowercase for words
- Inserting a number randomly in the word
- Placing numbers at the beginning and the end of words
- Putting the same pattern at both ends, such as <foobar>
- Replacing letters like <o> and <l> with numbers like <0> and <1>
- Punctuating the ends of words, such as adding an exclamation mark <!>
- Duplicating the first letter or all the letters in a word
- Combining two words together
- Adding punctuation or spaces between the words
- Inserting <@> in place of <a>

Educating end users on these tactics underscores the importance of creating long passwords (at least 19 characters) and applying multiple deviations, rather than something simple like just capitalizing the first letter.

InformationWeek DarkReading, "How Hackers Will Crack Your Password," 1/21/2009: http://www.darkreading.com/risk/how-hackers-will-crack-your-password/d/d-id/1130217[4]

Nine Tips to Strengthen Password Security

1. Change passwords annually.
2. Use different passwords for each login credential.
3. Avoid generic accounts and shared passwords.
4. Conduct audits periodically to identify weak/duplicate passwords and change as necessary.
5. Pick challenging passwords that include a combination of letters (upper and lower case), numbers and special characters (e.g. <$>, <%> and <&>).
6. Avoid personal information such as birth dates, pet names and sports.
7. Use passwords or passphrases of 19+ characters.
8. Use a Password Manager where users need just one master password.
9. Don't use a browser's auto-fill function for passwords.

The Two Factor Authentication Requirement

Two-factor authentication, is a way to double confirm an end user's identity. After the end user successfully logs in, they receive a text message with a passcode to then input in order to authenticate their ID.

This approach makes sure that end users not only know their passwords but also have access to their own phone. Two-factor authentication works well because cybercriminals rarely steal an end user's password and phone at the same time. All remote access and web portals should be set to require users to use two factor authentication.

Chapter 4
Mobile Security

Mobile Threats Jeopardizing Company Data

Mobile security is increasingly becoming a big concern as more and more companies adopt Bring Your Own Device (BYOD) environments, which allow end users to connect to corporate networks through their own (often multiple) devices. Even in cases where a business does not offer BYOD, end users often find a way to log onto business networks on their own.

With personal devices accessing corporate networks, businesses must now protect endpoint devic- es that are not completely under their control, which opens up the business to greater risk. Trying to gain control over personal devices also presents the challenge of making sure the company does not infringe on personal apps and information employees store on their own devices.

Mobile Device Security Challenges

- Lost, misplaced or stolen devices—remote wiping them quickly is key to protecting sensitive business and personal information.
- Mobile malware—hackers are now turning their attention to mobile devices and executing successful breaches through text messages. Android markets can be set up by anyone looking to sell malicious software to unsuspecting customers. Note: While mobile malware affects Androids more than IOS, a few exploits exist for Apple products as well.
- Unsecure third-party apps—if breached, they can serve as a gateway to other apps on a device and the device operating system, where security controls can be manipulated.
- Files with sensitive information accidentally emailed to an unauthorized party or posted online— once something is sent, it's out there forever.

Employees that utilize unsecured public Wi-Fi are another area of concern. Hackers in the vicinity of or on the same network can overtake a device without the end user even being aware, capturing sensitive data in transit. The end user can then become the victim of a man-in-the-middle attack, also referred to as hijacking. The hacker leverages the device so that it turns into an invasive device against other unsuspecting end users.

How Employees Can Secure Their Mobile Devices

Set a PIN or passcode:

This is the first line of defense—if someone wants to access the device, they first need to break the code. This is not an easy task and can operate as a deterrent against theft. Some device manufacturers also provide the option to automatically wipe the device after a few unsuccessful attempts at the passcode or PIN. So even if a phone is stolen, information cannot be accessed.

Use remote locate tools:

Several software solutions help locate lost or stolen devices through GPS and geofencing capabilities. Apple offers a service like this for mobile devices aptly named Find my iPhone. For Android users, the Android Device Manager offers these services, and Windows mobile users have this same option from the Windows Phone website. Similarly, many third-party applications are available in each of the app stores.

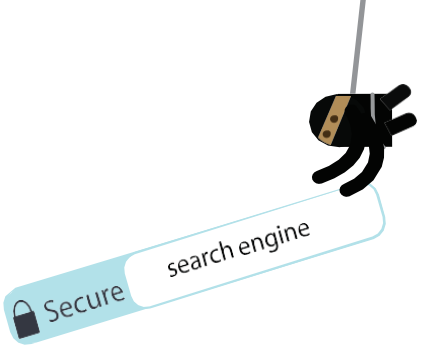
Keep devices clean:

Phones are mini-computers, and just like "big" computers, they need to be cleaned up from time-to-time. Utilizing an antivirus and malware scanner is always a good idea. Malware can compromise information stored on mobile devices and has a snowball effect that continuously piles up until it slows downs or stops the device.

Mobile Device Management (MDM) solutions help businesses and their employees apply these best practices by providing the ability to remotely wipe any devices that are lost or stolen. Such solutions also isolate personal apps from corporate apps in separate digital containers so that personal information remains private, and when an employee leaves the company, only their corporate apps and data are deleted while their personal apps and data are left intact.

By deploying an MDM platform, businesses can also enforce the use of passcodes to access devices, and they can apply geofencing capabilities that allow a lost device to be more easily located. End users can also be restricted to using only the corporate apps for which they have proper authorization. MDM also protects devices from jailbreaking and rooting—where hackers try to gain access to the operating system to open security holes or undermine the device's built-in security measures.

Chapter 5
Secure Website Browsing



The Top Browser Threats

When end users venture out onto the Internet, it's easy to get tangled up in the vast web of threats lurking on many website pages. Some of them are readily apparent, but others are well hidden.

Malvertising—a form of malicious code that distributes malware through online advertising—can be hidden within an ad, embedded on a website page, or bundled with software downloads. This type of threat can be displayed on any website, even those considered the most trustworthy. According to security firm RiskIQ, malvertising increased by 260% in the first half of 2015 compared to the same timeframe in 2014.5

Social Media Scams -- Hackers have created a playground of virtual obstacles across all the major social media sites. According to an article in The Huffington Post, some of the most common Facebook hacks and attacks include click-jacking, phishing schemes, fake pages, rogue applications and the infamous and persistent Koobface worm, which gives attackers control of the victim's machine while replicating the attack to everyone on their Facebook contact list.

Twitter isn't immune to security issues either. Since the microblogging site is both a social network and a search engine, it poses extra problems. According to CNET News, just 43 percent of Twitter users could be classified as "true" users compared to the other 57 percent, which fell into a bucket of "questionable" users. Among the things to watch for on Twitter are direct messages that lead to phishing scams and shortened URLs that hide malicious intentions.

Website Browsing Best Practices for Employees

- Be conservative with online downloads.
- Beware antivirus scams.
- Interact only with well-known, reputable websites.
- Confirm each site is the genuine site and not a fraudulent site.
- Determine if the site utilizes SSL (Secure Sockets Layer), Don't click links in emails—go to sites directly.
- Use social media best practices.

As for **Web-based exploits**, Internet websites are now the most commonly-used angles of attack, most often targeting software vulnerabilities or using exploits on the receiving client. This makes keeping up-to-date browsers paramount for all employees.

ComputerWeekly, "BlackHat 2015: RiskIQ Reports Huge Spike in Malvertising," 8/24/2015: http://www.computerweekly.com/news/4500251077/BlackHat-2015- RiskIQ-reports-huge-spike-in-malvertising5

Chapter 6
Security as Part of IT Strategy

How Cybersecurity Affects Your Business

Cybersecurity isn't just a matter of compliance, although customer requirements – for regulations such as FFIEC, HIPPA, PCI, DFAR and ITAR – often drive company investment in security. Businesses should recognize that there is value in their information and view security as a strategic initiative. To start assessing possible risk, businesses need to first analyze what information they possess, and what would be at risk if it was lost. The loss of intellectual property and operational data could result in loss of competitive advantage. Compromised employee information could result in legal exposure. The repercussions of lost financial data or unauthorized access to finances could have far reaching results that extend from loss of customer confidence to the financial stability of the business.

Partnering with a Managed Services Provider (MSP) that provides IT strategy along with IT department service can bolster your cybersecurity defenses. Human error is still highly dangerous, and many employees grow complacent at some point as they fail to follow best practices, but companies that offer fully managed IT services work proactively to mitigate risk and damage, while focusing IT activity and investment on your business goals.

When cybersecurity is part of your IT strategy, you begin to view it as more than just a matter of technology, and more than just a matter of compliance. The right managed IT service company will bring IT leadership and cost effective access to cutting edge resources that will allow security to be a function that makes your business better.

Conclusion:
Education and Technology - A Winning Cybersecurity Combination

As your business begins the journey to enhance its cybersecurity posture, it all starts with educating your employees. The tips provided within this E-Book along with some basic common sense can go a long way in making sure sensitive information does not fall into the wrong hands. Succeeding in applying the necessary cybersecurity measures is paramount to your long-term business success. In today's world of advanced hackers, who revel in breaching corporate networks, confidential information will always be at risk. Businesses must take the necessary steps to protect their intellectual property, their confidential information and their reputations while also safeguarding their employees, customers and business partners.

SCHEDULE A CONSULTATION

About The Author

Trusting your business can run smoothly with technology seems impossible when your current IT provider is slow to respond and the guidance is reactive. An IT strategy needs to be effective, support growth, and help get your business where it needs to be.

At Thriveon, we believe current IT methods aren't good enough—period. Your managed IT provider should be doing more than just patching issues and managing the day-to-day. They should be proactively preventing issues altogether, before they disrupt your people, and guiding you on the changes to make your business more efficient.

Back in 2005, your struggles were our struggles. We knew we needed a different solution, and so we built one. For the last 15 years, we've deployed an IT approach that supports and guides your business's entire technology spend, including software, hardware, and services so your business can do more with less. We help align your company to best practice standards with a 500-point inspection, reducing security issues and vulnerabilities by 90%, and proactively eliminating risks before they become a problem. It's time for a solid IT strategy to support your business growth and enable you to scale your business the right way.