This white paper addresses the key security threats that organizations must address, and how you and your fellow users can become a much stronger line of defense that can prevent many of these threats from penetrating corporate networks. The white paper was sponsored by ThinkHR, a brief overview of which is included at the end of the paper.
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why Should You Care About Cybersecurity?</td>
<td>3</td>
</tr>
<tr>
<td>You Can Defend Against Threats</td>
<td>5</td>
</tr>
<tr>
<td>Phishers Are Trying to Fool You</td>
<td>10</td>
</tr>
<tr>
<td>Your Mobile Device Is a Big Security Risk</td>
<td>14</td>
</tr>
<tr>
<td>Poor Authentication Is Risky</td>
<td>19</td>
</tr>
<tr>
<td>How To Defend Yourself</td>
<td>21</td>
</tr>
<tr>
<td>How Should You Deal With Viruses, Malware and Ransomware?</td>
<td>23</td>
</tr>
<tr>
<td>Social Media Is Another Big Problem</td>
<td>25</td>
</tr>
<tr>
<td>How To Defend Yourself</td>
<td>27</td>
</tr>
<tr>
<td>Summary and Conclusion</td>
<td>28</td>
</tr>
<tr>
<td>About Osterman Research</td>
<td>30</td>
</tr>
<tr>
<td>About ThinkHR</td>
<td>30</td>
</tr>
</tbody>
</table>
Why Should You Care About Cybersecurity?

You should care about cybersecurity even if you know nothing about the details of malware, phishing, Trojan horses, spam, advanced persistent threats, hacking, watering hole attacks, malvertising, man-in-the-middle attacks, botnets, copycat mobile apps or any of the other really bad things that can happen when you use email, the Web, social media, instant messaging and other communication and collaboration systems.

Here’s why:

You...

are the primary line of defense in preventing really bad stuff from happening in your company and to yourself.

There is nearly a one in four chance...

that you will mistakenly click on a phishing email.

One click on a phishing email...

could cost your firm $377 per employee.¹

A single trojan horse exploit...

caused the State of California to shut down a business a few days after the attack occurred.¹

One stolen laptop...

from the car of an HR professional who worked for Godiva Chocolatier revealed the names, addresses, Social Security numbers and drivers’ license numbers of other employees.¹

Things have changed over the past few years... cyber criminals are now focusing increasingly on you and your fellow users as the weak link in the security chain.
User Best Practices Are Essential

A solid and well-designed security infrastructure will protect against malware and other threats using a layered approach at various levels: desktops, laptops, mobile devices, servers, gateways and the cloud. Users have always been a key part of any security infrastructure, since a user not clicking on a link in a phishing email or not opening a malicious attachment, for example, will often thwart the ability for cyber criminals to penetrate corporate defenses.

You and Your Fellow Users Are Now the Target

However, things have changed over the past few years. Much of the server-, gateway- and cloud-based security infrastructure has become quite effective at filtering out a substantial proportion of malicious content. The result has been that cyber criminals are now focusing increasingly on you and your fellow users as the weak link in the security chain.

This is because security awareness training to help you understand how to deal with sophisticated cyber threats has not kept pace with advancements in security technology. While you and your fellow users can be effective at preventing the infiltration of threats into your corporate networks, most users do not receive sufficient training and so are not sufficiently skeptical about the content they receive in email, via social media, etc. The result is that cyber criminals are using a variety of techniques—often with a great deal of success—in penetrating corporate defenses, as shown in Figure 1.

In order to reduce the impact of the growing variety of threats that can infiltrate corporate networks, you and your fellow users must follow a variety of best practices as a first line of defense against data breaches, malware infiltration and various other security risks.

Figure 1: Percentage of Organizations That Have Been Infected by Various Threats

Source: Osterman Research, Inc.
You Can Defend Against Threats

Networks and Data Assets Are Under Attack

Corporate networks in organizations of all sizes are under siege by a growing number of increasingly sophisticated attacks from cyber criminals across the world. For example:

› The Privacy Rights Clearinghouse (PRC) maintains a database of data breaches dating back to April 2005. Since that time, PRC has chronicled nearly 4,800 data breaches and the breach of more than 895 million records.

› Symantec found that the number of data breaches increased by 23% during 2014 compared to the previous year.²

› McAfee Labs saw a 165% increase in new ransomware and a 317% increase in samples of Adobe Flash malware during the first quarter of 2015.³

› During the 14 months ended December 31, 2014, Business Email Compromise (BEC, or CEO Fraud) scams had created 2,126 victims generating nearly $215 million in losses.⁴

› A major survey found that 19% of organizations in the United States lost anywhere from $50,000 to $1 million to cyber-related fraud during 2014.⁵

There Are Lots of Weak Points That Cyber Criminals Can Exploit

A key reason for the growing vulnerability of businesses to various types of cyber attack is the growing attack “surface” that businesses present to cyber criminals—namely, the number of possible entry points for malware and other exploits.

Anytime you access resources on the corporate network, you risk becoming a victim.

For example, you use a number of company-provided solutions, such as corporate email, corporate social media, smartphones, tablets, laptops, desktop computers, collaboration systems like SharePoint, USB thumb drives, various cloud-based solutions, and a number of other applications and tools. Each of these can serve as an entry point for malware, hacking attempts and other infiltration by cyber criminals.

You probably also use your own devices and applications to access company systems and data sources, such as corporate email and file servers. These personally owned solutions include smartphones, tablets, personal Webmail (often used when the corporate system is down or when users need to send very large files), social media accounts, file sync and share tools like Dropbox,
home computers, mobile apps, and various cloud-based applications. These also represent ingress points for various types of threats and are often a more serious problem because their use is not as well controlled by IT (if they’re controlled at all).

Growing use of email and other communication and collaboration platforms contribute to the growing attack surface, as well, by offering a larger number of opportunities for phishing attempts and other types of infiltration to corporate networks. For example, the more emails that you receive, the more likely that a cyber criminal will be able to eventually penetrate your corporate defenses.

What Types of Threats Are Being Aimed At You?
You and your company are being targeted with a variety of threats, ranging from seemingly innocent infiltrations like spam that create storage problems and general annoyance, to highly targeted email attacks that can create major breaches of sensitive or confidential information. Among the range of threats—as well as solutions that can create an infiltration point for a cyber criminal—you need to consider are the following:

PHISHING ATTACKS
Phishing emails are relatively unfocused email messages that are designed to collect sensitive information from you, such as your login credentials, credit card information, Social Security numbers and other valuable data. Phishing emails pretend to come from trustworthy sources like banks, credit card companies, shipping companies and other sources with which potential victims already have established relationships. More sophisticated phishing attempts will use corporate logos and other identifiers that are designed to fool potential victims into believing that the phishing emails are genuine.

SPEARPHISHING EMAILS
Spearphishing emails are targeted phishing attacks that are generally directed at a small group of potential victims, such as senior individuals within your company. Spearphishing emails are typically focused on one company or affinity group (such as an industry organization), reflecting the fact that a cyber criminal has studied his or her target and has crafted a message that is designed to have a high degree of believability and a potentially high open rate.
CONSUMER FILE SYNC AND SHARE TOOLS
Consumer file sync and share tools like Dropbox, Microsoft OneDrive and Google Drive, among many others, allow you to make your files available on all of your desktop, laptop and mobile platforms. While these tools are quite useful and generally work as intended, they represent a key ingress point for malware. For example, when you access your corporate files on your home computer—and assuming you’re like many home users and don’t keep your anti-virus software current—you can inadvertently infect these files with malware. When the files are synced back to your desktop or laptop computer at work, malware can readily infect the network because it may have bypassed corporate email, Web gateway and other defenses. In an alternative infection scenario, when you work from home your infected files can be sent directly to a business partner or client without the files ever having passed through your corporate security system.

REMOTE USERS WITH ACCESS TO CORPORATE RESOURCES
Anytime you access resources on the corporate network, you risk becoming a victim. For example, if you access a corporate Webmail system, such as Outlook Web Access that is not accessed via a virtual private network (VPN), or your laptop computer becomes infected and later is connected to the corporate network, you can spread malware onto the corporate network. This is becoming a serious problem for most organizations, as users employ personally owned devices like their own smartphones, tablets and other devices in a workplace setting.

WATERING HOLES
Watering holes are a type of social engineering attack in which cyber criminals will identify Web sites that they would like to infiltrate and that you might visit on a regular basis. Cyber criminals will infect these sites with malware, the goal of which is to infect members of the affinity group.

MALICIOUS INTERNET ADVERTISING (MALVERTISING)
Malvertising is designed to distribute malware through advertising impressions on Web sites. An Online Trust Alliance brief shows how a single malvertising campaign can generate 100,000 impressions. 

Ransomware is a particularly malicious form of attack in which a cyber criminal can encrypt all of the files on your hard disk and then demand ransom for access to a decryption key.
USER ERRORS
Users will sometimes inadvertently install malware or compromised code on their computers. This can occur if you install ActiveX controls, download a codec, install various applications that are intended to address some perceived need (such as a capability that IT does not support or that you feel you should have), or when you respond to scareware attempts. Scareware is a particularly dangerous type of malware because it preys on users who are actually trying to do the right thing—i.e., protect their platforms from viruses and other malware.

MOBILE MALWARE
The increasing use of smartphones and tablets, particularly personally owned devices, is increasingly being exploited by cyber criminals. For example, Alcatel-Lucent found that 16 million mobile devices were infected with malware during 2014, an increase of 25% from 2013. This represents an infection rate of 0.68%, meaning that in an organization of 100 employees, each of whom has an average of 1.5 mobile devices, there will be a total of 10 infected mobile platforms at any given time. The vast majority of infections impact Android devices—the Alcatel-Lucent research suggests that fewer than 1% of iPhone and BlackBerry devices are infected with malware.

COMPROMISED SEARCH ENGINE QUERIES
Valid search engine queries can be hijacked by cyber criminals to distribute malware when you perform Web searches. This type of attack relies on poisoning search queries, resulting in the display of malware-laden sites during these searches. Search engine poisoning is particularly effective for highly popular search terms, such as information on celebrities, airline crashes, natural disasters and other “newsy” items. However, these attacks can occur on any Web site.

MOBILE COPYCAT APPS
Many mobile app developers distribute their wares through vendor-based and third party stores that offer varying levels of security, much of it inadequate. Some app stores—such as the Apple App Store—are highly secure operations and require that developers satisfy rigorous standards before their apps can be offered. Others’ standards, however, are often less stringent and create the opportunity for serious security risks. The result is that many third-party app stores are susceptible to a number of security and related problems like the distribution of copycat apps and malware. If you download from one of these third-party stores, you are more likely to get infected.

BOTNETS
Botnets are the source of many successful hacking and phishing attacks against high-profile targets. For example, the US Senate, Sony, Citigroup, Lockheed Martin, the International Monetary Fund, RSA, and Northrup Grumman have all been victimized by botnet attacks. This has resulted in millions of records being exposed that will result not only in the disclosure of personal and sensitive information, but also lawsuits and other expensive remediation efforts.
RANSOMWARE
Ransomware is a particularly malicious form of attack in which a cyber criminal can encrypt all of the files on your hard disk and then demand ransom for access to a decryption key. Victims who choose not to pay the ransom within a short period of time will have their files remain encrypted permanently. Cryptolocker, one of the common variants of ransomware, typically extorts a few hundred dollars per incident and is normally delivered through email with a PDF or .zip file disguised as a shipping invoice or some other business document. In case you’re tempted to think that ransomware is just an annoyance and not a life-or-death issue, think again: in February 2016, a southern California hospital had to pay $17,000 in ransom to regain access to its files and communications systems.

HACKING
This is a form of cyber attack in which cyber criminals use a number of techniques in an attempt to breach corporate defenses. An example of a successful hacking attack is the incursion against Sony Pictures that may have been carried out by an operation of the North Korean government.

You Are the First Line of Defense
It is critical for your company’s decision makers to realize that you and your fellow users are actually the first line of defense in the overall security infrastructure. Secure Web gateways, antivirus tools, malware scanners, spam quarantines and other capabilities are important elements in defending against a growing variety of threats, but you are the vital link in the security chain that determines whether or not an attack will be successful. For example, even the best filtering technologies deployed at multiple locations will not be able to stop all phishing attempts from reaching you. Consequently, if you can recognize such an attempt because you have been trained to do so, and then take the appropriate steps to deal with it, you can protect against the ingress of malicious content.
Phishers Are Trying To Fool You

What Is Phishing?
A phishing attack is typically a bogus email, Web page or social media post generated by a cyber criminal that pretends to be from a legitimate source. The goal of a phishing attack is to trick you into sharing sensitive or confidential information, such as login credentials, credit card numbers, financial account information or similar types of information.

Phishing is successful if it can fool you into believing that what you’re seeing is genuine, particularly when it coincides with your expectations. For example, during your company’s open enrollment period for healthcare benefits, it’s logical that you would receive an email about your company’s benefits package. Phishers know this and exploit this to their benefit by sending you messages that you would naturally expect to receive.

An important variant of phishing is spearphishing. While the ultimate goal of a spearphishing attack is identical to a phishing attack—i.e., stealing financial or other valuable information—a spearphishing attack is much more targeted, typically aimed at a small group of people within your company, such as C-level executives, members of a design team or others with highly sensitive information. A variant of spearphishing is “whaling,” which tends to be even more highly targeted, sometimes focused on your CEO, COO or some other individual within a company. Cyber criminals who launch spearphishing or whaling attacks are typically after the most sensitive types of information, such as the login credentials to a company’s financial accounts.
Some Real-World Examples

Phishing and spearphishing can cost an organization hundreds of thousands of dollars and can actually put your company out of business. Here are some examples:

› An employee of Penneco Oil Company in Delmont, PA received a phishing email and either clicked on a link or opened an attachment within the email. This installed a keystroke logger that allowed cyber criminals to transfer almost $2.2 million from the company’s financial accounts to a bank in Russia, and $1.35 million to a bank in Belarus. Cyber criminals attempted to transfer another $76,000 to a bank in Philadelphia shortly thereafter, but were not successful.\(^\text{10}\)

› CEO fraud, a type of spearphishing attack, victimized The Scoular Company, an Omaha-based commodities trader. The controller of Scoular received an email that was supposedly from the company’s CEO, instructing him to wire $780,000 to a bank in China, but instead the request came from a cyber criminal with email addresses in several different countries and servers operating in Moscow. The controller believed that the email was genuine and was instructed to keep the transaction secret so as not to violate Securities and Exchange Commission regulations. The initial request was followed by two more requests to transfer a total of $16.4 million, bringing the total theft to $17.2 million.\(^\text{11}\)

› Efficient Service Escrow Group, a California-based escrow firm, was the victim of a Trojan malware infiltration that resulted in three wire transfers from their financial accounts to banks in Russia and northern China totaling $1.5 million. The transfer of $432,000 to the Russian bank was recovered, but the transfer of $1.1 million to the bank in China was not. California state law requires immediate disclosure of loss of funds for title and escrow companies, and so the company was given three days to replace the missing funds. Because they were not able to do so, the State of California shut the business down.

While these may seem like unusual examples, unfortunately they are not. Verizon analyzed 150,000 phishing emails from its partners and found that 23% of recipients open the phishing emails they receive and 11% open the attachments contained within them. Moreover, the length of time between the launch of a phishing attack until the first recipient responds to it is 82 seconds; one-half of phishing messages are opened in less than one hour.\(^\text{12}\)

While email is the most common venue for phishing attempts, cyber criminals can also hijack pages on a Web site and make them appear to be valid, or post links on social media that will instruct users to “like” or otherwise interact with a social media site.
How To Defend Yourself

While cyber criminals are often very good at disguising their phishing emails, Web pages and social media posts, there are things that you can do to reduce the likelihood of becoming a victim:

**BE SKEPTICAL**

First and foremost, be skeptical of any email, Web page or social media post that appears to be even remotely suspicious, makes an offer that is too good to be true, or contains strange information. For example:

In the bogus iTunes message shown on Page 10, the date on the email is January 8, 2016, but it was received on February 8, 2016. If you have ever ordered content from iTunes, you would know that Apple almost always emails receipts within two or three days from the purchase date. Moreover, the URL in the link near the bottom of the email does not match the URL in the tag that hovers over the address when the cursor is placed above it. An even more careful observation of the email reveals that the Apple logo appears slightly narrower than the Apple logo in a genuine iTunes receipt.

The Facebook post at right is slightly more obvious. For example, if you saw this post in Facebook you should question why Southwest Airlines would refer to themselves as “South West Air,” or why the airline would be giving away 775 first class flights and $5,000 in cash simply for “liking” their page. Plus, Southwest does not offer first class seats, probably would not advertise using an aircraft with their old color scheme, and they most certainly would not have first class seats with the logo of Malaysia Airlines on the television monitor.

Since emails are the most common method for distributing phishing attacks, it’s important for you to ask some questions about any email you receive.

Figure 4: Example of a Bogus Facebook Page
Source: Facebook
ASK QUESTIONS
Second, since emails are the most common method for distributing phishing attacks, it’s important for you to ask some questions about any email you receive. Here are some good questions to ask:

- Do you recognize the sender’s email address?
- Do you recognize anyone else copied on the email?
- Are others in the email seemingly from a random group of people, or do these recipients’ last names all begin with the same letter?
- Is the domain in the email address spelled correctly or is it simply close to the actual URL (e.g., bankofamerica.com vs. bankofarnerica.com).
- Would you normally receive an email from this individual?
- Does the subject line make sense?
- Is the email a response to an email you never sent (e.g., does it begin with “re:”)?
- Does the URL in the email (if there is one) match the URL in the tag when you hover over the link with your mouse cursor?
- Does the email contain an attachment that does not make sense in the context of the email or sender?
- Does the attachment end in “.exe,” “.zip” or some other possibly dangerous attachment type?
- Did you receive an email at an unusual time, such as 3:00am on a Sunday morning?
- Is the sender asking you to keep the contents of this email or any requests within it a secret?
- Does the email contain spelling or grammatical errors?
- Is there even a hint of extortion in the email, such as a request to look at compromising or embarrassing photos of you or someone else?

BE VERY CAREFUL WHEN REVIEWING YOUR QUARANTINED MESSAGES
If an email that seems to be valid has been captured by a spam quarantine, it is essential to be extremely careful before assuming it was mistakenly identified as spam and bringing the email out of quarantine. These “false positives” are not the norm, and so the spam quarantine that has captured a phishing email probably did so correctly.

DO NOT CLICK
Finally, you should never click on a link in an email or open an attachment until you are absolutely certain that the link or attachment is valid.
Your Mobile Device Is a Big Security Risk

Your Smartphone Is Full of Data

The growing use of mobile devices creates an enormous security risk given that 66% of employees use their own devices for work-related purposes. Your mobile devices contain a significant proportion of your company’s data, including email, files, contacts, calendar appointments, customer information and other potentially sensitive and confidential data. As shown in Figure 5, users’ smartphones and tablets contain 6% of the typical company’s data; when laptops are added to the mix, however, more than 20% of corporate information is housed on a mobile device.

![Bar chart showing distribution of corporate data by location](image)

Figure 1: Distribution of Corporate Data by Location
Source: Osterman Research, Inc.
The Information On Your Smartphone or Tablet Can Be Easily Compromised

One of the fundamental problems with your mobile devices is the thing that makes them so useful: their mobility. This means that your smartphone and tablet contain sensitive or confidential corporate information that can create a data breach if they are lost or stolen. Here are a few examples of what can happen:

- In January 2016, New West Health Services in Kalispell, MT revealed that one of its laptops went missing, breaching 28,209 records.¹⁵
- An employee of Buyers Protection Group in Alpharetta, GA had a laptop stolen during a large-scale burglary of cars, revealing an unknown number of customer records.¹⁶
- Consumer Reports found that 4.5 million smartphones were stolen or lost in 2013, up dramatically from 2.8 million in 2012.¹⁷

In addition to the problem of theft or loss of mobile devices are the following issues that can result in data breaches and other problems:

- A growing proportion of mobile devices are personally owned—an Osterman Research survey conducted during January 2016 found that for 39% of employees, the primary work-related smartphone they use is their personally owned device.¹⁸ This means that a substantial proportion of mobile devices—and the corporate data contained on them—is under the control of you and your fellow employees, not the IT department.

- Many users do not password-protect their personally owned devices or know how to delete all of the data from them if they are lost. An unprotected mobile device that cannot be wiped can result in a data breach if it is lost or stolen.

Even if the data has not actually been breached as the result of a loss or theft, the company whose data was lost must still report the breach depending on the type of data that was compromised. For example, loss of sensitive or confidential health care patient information in excess of 500 records must be reported to the U.S. Department of Health and Human Services, and 47 of the 50 U.S. states require reporting of any breach of unencrypted information to its owners in those states.

First and foremost, every mobile device you use should be password-protected so that access to any sensitive or confidential stored on it will not be easily accessible.
Many users are tempted to access publicly available Wi-Fi connections, particularly when using tablets or laptops that do not have a cellular connection. Public Wi-Fi hotspots, available at locations like coffee shops, airports and restaurants, are notoriously subject to hacking by cyber criminals. When users enter their login credentials to access corporate email, social media and other sensitive sites, hackers can easily steal these credentials to gain access.

Many users mistakenly download “copycat” applications to their mobile devices that allow cyber criminals to steal sensitive information. These apps are designed to look and operate like legitimate apps, but instead are intended for a variety of malicious purposes. For example, a developer can easily disassemble an existing app and repackage it so that it looks similar or identical to a legitimate one, but the app will include code that will add spam or other advertising in the app interface, send expensive SMS messages that will add charges to the victim’s wireless bill, or implement a capability to steal login credentials. As just one example, NQ Mobile reported a copycat mobile app designed to impersonate the legitimate NetDragon 91 Assistant app. When installed, the copycat app sends premium SMS messages that will appear as additional charges on victims’ wireless bills.19
How To Defend Yourself

There are a number of things that users can do to mitigate the risks associated with the use of mobile devices when used for work-related purposes:

USE PASSWORD PROTECTION
First and foremost, every mobile device you use should be password-protected so that access to any sensitive or confidential stored on it will not be easily accessible.

DISABLE AUTO USERNAME AND PASSWORD COMPLETION
You should disable automatic username and password completion. While this makes the use of a mobile device somewhat more tedious, it can reduce the likelihood of sensitive or confidential information being accessed by someone who finds or steals an unprotected mobile device.

ALWAYS INSTALL SECURITY UPDATES
You should always elect to install updates–many of which are focused on improving security–as soon as they are available. A failure to do so can leave a mobile device more vulnerable to security threats than is necessary.

BE SURE YOU CAN WIPE YOUR DATA
Ensure that your device can be wiped of all data if it is lost or stolen. While IT departments can generally do this for company-supplied devices, if you employ your own device you should know how to do this.

BE VERY CAREFUL WHEN USING PUBLIC WI-FI NETWORKS
You should be very careful when accessing public Wi-Fi networks. Networks that do not require a password are highly insecure and even networks that require only a WEP password can be easily hacked. Wi-Fi networks that require the use of a WPA or WPA2 password are not invulnerable, but are much more secure.

USE A HOTSPOT ON A TRUSTED PHONE OR AN ENCRYPTED VPN
If possible, when connecting a laptop or tablet to the Internet, you should employ a hotspot on a trusted mobile phone, or use an encrypted VPN when using a public Wi-Fi hotspot.

DISABLE FILE SYNC AND SHARE
If you connect to any public network, disable all file sync and share tools, such as Dropbox, to reduce the likelihood of a data breach.
BE CAREFUL WHEN ENTERING SENSITIVE INFORMATION
When you access a Web site that requires entering sensitive or confidential information, do so only on Web sites that are encrypted (i.e., the URLs begin with “https” and that contain an icon of a lock in the URL bar and a green URL).

Figure 8: Example of an Authentic and Secure URL  
Source: PayPal

USE ONLY “SAFE” STORES
When downloading mobile apps, use only stores with robust security controls, such as the Apple Store or Google Play. Many third party stores do not have rigorous security controls and can serve as a host to copycat or other malicious apps.

SEE IF YOU CAN GAIN ACCESS TO SEGMENTATION TECHNOLOGIES
While you probably don’t have control over technologies installed on a mobile device that can segment personal and corporate data on the same device, you can ask your IT department to at least investigate them. These technologies will permit the corporate “side” of the mobile device to be wiped by IT if the device is lost or stolen (or when an employee leaves the company), while not affecting your personal information.
Poor Authentication Is Risky

What Are We Talking About?
Authentication is simply the process of verifying that you are who you say you are when attempting to access a system. The most common form of authentication is a username and password combination, but there are a number of different authentication methods that can be used:

**TWO-FACTOR AUTHENTICATION**
This method of authentication requires two different verification modes to gain access to a system. For example, an automated teller machine (ATM) requires you to have something (an ATM card) and to know something (a Personal Identification Number, or PIN) in order to make a transaction.

**OUT-OF-BAND AUTHENTICATION**
This access method uses two completely different communication modes to verify you. For example, upon successfully entering a username and password on a desktop computer, a system can then require you to enter a code that it sends to your mobile device.

**CHALLENGE/RESPONSE**
This method requires you to answer questions that you previously entered into a system. For example, many banks require you to a) enter your username, b) answer one of several questions about your personal life, and c) provide your password. If you cannot answer correctly, you are not given the opportunity to enter your password.

**IMAGES OR PATTERNS**
Some systems require you to enter letters and/or numbers that are provided in an image after you have entered your username and password. This method of authentication, also known as CAPTCHA, can prevent robots or automated dictionary attacks from gaining access to a system because these tools are typically not capable of identifying text in images.

**BIOMETRICS**
These methods require you to scan your fingerprint, iris, face, finger length, voice, typing rhythm or some other unique, biological characteristic that is unique to you when attempting to access the system. These systems have the distinct advantage of being difficult to spoof by unauthorized parties, but they can result in false rejections. Some systems are quite sophisticated—for example, the biometric authentication used in Microsoft Windows 10 can detect the blood flow in your face and cannot be fooled even by your identical twin.
Weaknesses In Current Authentication Schemes

While authentication is required in virtually every corporate system, there are a number of weaknesses in some current authentication schemes and/or the way they are implemented by many users and IT departments. Addressing these vulnerabilities is essential for any organization, since 75% of network intrusions are the result of stolen or weak credentials.

› Many users employ extremely weak passwords that are easy for cyber criminals to guess. For example, Splash Data found that the five most common passwords employed in 2015 were “123456,” “password,” “12345678,” “qwerty” and “12345.”

› Most users do not change their passwords on a regular basis and are not forced to do so by a corporate system. The result is that systems are increasingly vulnerable over time simply because the same password is exposed to cyber criminals for a longer period.

› Most users employ the same password to access multiple systems—a survey of users in the United States and the United Kingdom found that nearly 75% of users do so. While this practice makes it easier for users because they need to remember fewer passwords, it also makes it easier for cyber criminals, since hacking into one system by determining a user’s password gives them access to several other systems.

› In some situations, users will share the same login credentials with others, particularly for systems like FTP servers that are not frequently accessed. This makes data breaches easier because multiple people have the same login credentials and because these credentials are often not changed when a user leaves the company.

You should always use strong passwords when accessing a corporate system.
How To Defend Yourself

There are a number of best practices that users should employ when accessing corporate systems:

EMPLOY STRONG PASSWORDS

You should always use strong passwords when accessing a corporate system. Typically, the longer the password and the greater the variety of characters it contains (upper case, lower case, numbers, punctuation, etc.), the stronger and more difficult it will be to hack.

To demonstrate the relationship between the strength of a password and the length of time required to crack it, we ran five passwords of various strength through the password checking site howsecureismypassword.net. The amount of time required for a desktop PC (performing four billion calculations per second) to randomly crack each password is shown in Figure 10.

<table>
<thead>
<tr>
<th>Password</th>
<th>Time to Crack</th>
<th>Character Combinations</th>
<th>Possible Combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>happy</td>
<td>&lt; One second</td>
<td>26</td>
<td>11 million</td>
</tr>
<tr>
<td>happy9</td>
<td>0.54 seconds</td>
<td>36</td>
<td>2 billion</td>
</tr>
<tr>
<td>happy99</td>
<td>19 seconds</td>
<td>36</td>
<td>78 billion</td>
</tr>
<tr>
<td>happy99K</td>
<td>15 hours</td>
<td>62</td>
<td>218 trillion</td>
</tr>
<tr>
<td>Happy99K)</td>
<td>275 days</td>
<td>77</td>
<td>95 quadrillion</td>
</tr>
</tbody>
</table>

Figure 10: Comparative Strength of Passwords

Source: Small Hadron Collider

Obviously, a hacker could probably make more educated guesses if he or she was attempting to crack your password, but the example above demonstrates that stronger passwords create more of a barrier for cyber criminals.

CHANGE YOUR PASSWORDS FREQUENTLY

While some systems and IT administrators force a change in passwords on a regular schedule, you should routinely change your password without prompting. Setting a calendar reminder, for example, to change passwords every 90 days can help to reduce the likelihood that your passwords will become compromised.
USE A UNIQUE PASSWORD FOR EVERY SYSTEM
The common practice of using the same password across multiple systems increases the
opportunity for a cyber criminal to hack one password and thereby gain access to multiple
systems. Best practice is to use a unique, strong set of login credentials for every system.

INTENTIONALLY USE WRONG INFORMATION FOR SECURITY QUESTIONS
Some systems, particularly those that ask users to answer a variety of security questions during
the initial set-up, will ask for information like your mother’s maiden name, the name of your first
pet, the city in which your parents were married, etc. Because this information might be requested
by a variety of systems, providing the “wrong” answer to these questions, and providing different
wrong answers for each system, can reduce the likelihood of a cyber criminal being able to respond
to security questions correctly.

EMPLOY AUTHENTICATION APPROPRIATE TO THE SENSITIVITY OF THE INFORMATION
In most cases, IT will establish the level of authentication required for you to access a system, but
you often have some control, particularly for personally-managed cloud applications and the like.
For example, Dropbox allows you to set up two-factor authentication that requires not only the
input of your username and password, but also a six-digit code that is sent to your mobile device.
This extra level of authentication, while not 100% secure, makes it more difficult for cyber criminals
to access your Dropbox account because they would need both your username/password
combination and your mobile device.

USE A PASSWORD MANAGER
For companies that have not implemented single sign-on capabilities, the use of a password
manager that will store login credentials is useful. These solutions allow you to create very
strong passwords without being required to remember them. Some operating systems, such as
later versions of Mac OS X, as well as some Web browsers, have built-in password management
capabilities, but there are numerous commercial packages available as well.
How Should You Deal With Viruses, Malware and Ransomware?

What Are We Talking About?

A virus is malicious code that can replicate itself with a variety of consequences, ranging from simple annoyance to theft of data and, in some cases, complete disablement of a computer. Similarly, malware is malicious code that is intended to steal data, record user activity (such as keystrokes), or cause a system to fail. Viruses and malware are typically created by cyber criminals for the purpose of infiltrating your computer, the databases you use, your file stores and other repositories of sensitive or confidential information, but they can also be part of a state-sponsored attack with more strategic objectives. The Stuxnet worm, for example, was a highly sophisticated piece of malware that was designed to infect a particular type of Siemens controller used in the Iranian nuclear weapons program.

Ransomware is a type of malware that can encrypt the data on your hard drive and then demand payment within a limited period of time for the decryption key. Without payment, the files become permanently inaccessible.

The Damage They Can Cause

Viruses, malware and ransomware can cause enormous damage. For example:

› One of the most damaging viruses was ILOVEYOU, written by two programmers in the Philippines. This virus, which was spread using phishing techniques, would overwrite files on victims’ computers, rendering them unbootable. The virus infected more than 45 million computers worldwide, and one estimate placed total damage from ILOVEYOU at $10 billion.\(^\text{23}\)

› Zeus is a particularly damaging type of malware that performs both keylogging and form grabbing, and was responsible for the theft of login credentials from a wide variety of Web sites, email systems, social media properties and bank accounts. Tens of millions of dollars have been drained from financial accounts using Zeus and its variants.

› Ransomware, the most common of which is CryptoWall, caused $18 million in losses for the 15 months ended June 2015 according to the FBI Internet Crime Complaint Center;\(^\text{24}\) the Cyber Threat Alliance estimates that CryptoWall 3.0 has cost victims up to $325 million.\(^\text{25}\) Victims typically pay anywhere from a few hundred dollars to as much as $10,000 to regain access to their encrypted files. Ransomware can be spread through various means, including phishing emails, but can also be spread through bogus software updates.

While nothing can completely prevent viruses, malware and ransomware from infecting a computer, there are some things you can do to significantly reduce the chance of infection.
How To Defend Yourself

While nothing can completely prevent viruses, malware and ransomware from infecting a computer, there are some things you can do to significantly reduce the chance of infection:

**KEEP YOUR SECURITY SOFTWARE UP-TO-DATE**

While a software update can potentially be bogus, it is essential to apply updates to operating systems, security software and other software as soon as possible after they are published (this is particularly true for plug-ins like Adobe Flash that are highly vulnerable to exploits). Vendors are continually updating and improving the security of these software systems, and so applying updates can prevent some types of infection.

**DON’T CLICK ON LINKS OR OPEN ATTACHMENTS**

It is essential never to click on links or open attachments from unknown or suspicious sources, since doing so can introduce viruses, malware or ransomware onto a computer and into a corporate network.

**NEVER USE USB FLASH DRIVES FROM UNKNOWN SOURCES**

USB flash drives help you to share files, take work home, or distribute content to customers and prospects. They are commonly handed out at trade shows and conferences, but are a common source of infection. For example, an analysis of 50 USB flash drives that were found on trains in and around Sydney, New South Wales found that two-thirds of them were infected with some form of malicious software. More recently, the control systems for two power generation facilities in the United States were infected with malware that had been introduced by USB flash drives.

**PERFORM REGULAR BACKUPS**

Finally, performing regular backups of all computer systems allows recovery from a virus, malware or ransomware infection. By reinstalling the operating system on an infected computer and restoring files from a pre-infection backup, you can go back to a point prior to the infection. While this may result in some data loss, it can restore a computer almost completely to a known good state.

Many social media accounts are hacked by cyber criminals. For example, one source estimates that 160,000 Facebook accounts are hacked on a typical day.
Social Media Is Another Big Problem

Social Media Use Is Widespread

The use of social media in the workplace is pervasive, not only by employees for their own use, but also for legitimate business purposes. For example, 73% of the organizations surveyed by Osterman Research in January 2016 employ Facebook for business purposes, 64% use LinkedIn, and 56% use Twitter, in addition to a variety of other social media platforms.

How Does Social Media Pose a Threat?

Social media can provide you with a number of important benefits that can help your company to become more efficient, help you to speed the decision-making process, and allow information to be shared in a way that is not possible or practical using other methods. However, the use of social media also represents a significant threat:

HACKED ACCOUNTS

Many social media accounts are hacked by cyber criminals. For example, one source estimates that 160,000 Facebook accounts are hacked on a typical day. Social media accounts can be hacked through phishing schemes, through the variety of third-party apps for which users give write access, or simple password cracking. The result of a hacked account may be nothing more than sending spammy messages, or it can be part of a malware distribution campaign.

MALWARE DISTRIBUTION

Social media platforms that limit the number of characters that can be sent, such as Twitter, necessitate the use of short URLs that can make it much easier for cyber criminals to disguise a link to a malicious site. Social media can also be the target of state-sponsored attacks. For example, in December 2015 Twitter issued a security alert to some users that they might have been "targeted by state-sponsored actors," the first alert of its type made by the company. Moreover, malvertising is on the increase and can infect leading social media properties. Proofpoint recently discovered a promoted Twittercard that can lead to installation of malware designed to steal Facebook credentials. 

SCAMS AND BOGUS OFFERS
Social media is also a breeding ground for all sorts of scams and bogus offers that can trick users into revealing sensitive information. One study found that 24% of Facebook advertisements were selling counterfeit products. As just one example, as of February 2016, Facebook has been hosting a bogus Web site for at least the past 15 months: the site for “South West Airline.” The Facebook page is clearly bogus, not only because it contains a URL for a domain that has not been registered, but also because the perpetrators of this fraud did not spell the name of the airline correctly. The page has been “liked” by nearly 3,000 people and it displays an offer that has been shared nearly 23,000 times.

CLICKJACKING
This practice involves burying various hyperlinks under legitimate content on a social media page. When a user clicks on what he or she believes to be a valid link, the result can be a malware download to the computer or distribution of the link to other contacts after clicking the “Share” or “Like” button.

The Biggest Problem Is Users
The core of the social media security problem is users who fail to be sufficiently skeptical of advertisements, too-good-to-be-true offers, or who are too willing to “like” or “share” posts. Add to this the problem of oversharing information on social media, thereby providing phishers and spearphishers with the information they need to increase their chances of success. For example, if you share your experience about XYZ Restaurant on Facebook and your profile is public, a cyber criminal can use this information to send you an email with the subject line, “Problem with your recent credit card charge at XYZ Restaurant.” Given that you were there recently, it makes sense that you would receive an email of this type, making you more likely to open it. Moreover, sharing too much information via social media can allow others to “connect the dots” about a merger, acquisition or some other business deal that would not otherwise have been revealed.
How To Defend Yourself

There are a number of things that you can do to increase the security of your experience and reduce the likelihood of malware infiltration, data loss or other problems:

DON’T OVERSHARE
Simply put, don’t share an excessive amount of information via social media. Not every dessert, vacation photo, medical condition or thought needs to find its way onto a social media page. Toward this end, it might be useful to limit who can see posts or access contact information on Facebook, Instagram and other social media properties. These controls are typically available in the settings of your social media account.

TURN OFF LOCATION SERVICES
Many social media platforms permit you to share your location, either manually or through geolocation services that will automatically post your location. Use of location information in social media posts can tell business colleagues about your multiple trips to Bentonville, Arkansas (which could strongly hint that your company is about to do a deal with Wal-Mart, for example). In an extreme example of the dangers inherent in automatically sharing location data, some US soldiers in Iraq posted photos on Facebook, not realizing that they had been geotagged. This provided insurgents with the data they needed to destroy four Apache helicopters.

TURN ON OUT-OF-BAND AUTHENTICATION
Many social media platforms permit the use of out-of-band authentication that will require entry of a code delivered to a mobile device when logging in from a new browser. This can reduce the likelihood that cyber criminals will be able to access your social media account.

BE CAREFUL WHEN CLICKING, LIKING OR SHARING
Finally, be careful when clicking on a link or sharing it. As noted, doing so could inadvertently distribute malware or spammy messages to others in your social media circle.
Summary and Conclusion

The attack surface for most organizations—i.e., the exposure they have to cyber attacks—is increasing because of the growing use of various types of communication, collaboration, content-sharing and other applications and devices employed by you and your fellow employees. While the tens of billions of dollars that companies have spent on cybersecurity have been effective at thwarting many threats, the result has been that cyber criminals are now increasingly targeting you and your colleagues because security awareness training has been lacking. Compounding the problem is that many users are just not as skeptical as they should be about what they receive in email or see on the Web or in social media.

To improve corporate security, every company should implement a program of security awareness training for their employees, contractors and others who interact with corporate systems and data sources to help you become a stronger line of defense for your organization.
PRACTICAL STEPS TO DEALING WITH PHISHING, MALWARE, AND OTHER THREATS TO YOUR BUSINESS

2. Symantec Internet Security Threat Report 20
6. https://www.otalliance.org/resources/advertising-integrity-fraud
7. Source: Alcatel-Lucent Motive Security Labs division
13. Source: KnowBe4 and Osterman Research, Inc.
15. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;sessionid=
17. http://nypost.com/2015/03/01/big-brother-2-0-160000-facebook-pages-are-hacked-a-day/
20. Completely Automated Public Turing Test to Tell Computers and Humans Apart
21. Source: Mobile Enterprise Applications and Solutions FutureScape
22. http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514
33. https://nakedsecurity.sophos.com/2012/05/08/facebook-clickjacking/
34. http://nypost.com/2015/03/01/big-brother-2-0-160000-facebook-pages-are-hacked-a-day/
About Osterman Research

Osterman Research provides timely and accurate market research, cost data, cost models, benchmarking information and other services to technology-based companies. We do this by continually gathering information from IT decision-makers and end-users of information technology through in-depth market research surveys. We analyze and report this information to help companies develop and improve the products and services they offer, and to help organizations make better decisions about their security, archiving and other capabilities.

For more information, visit ostermanresearch.com.

© 2016 Osterman Research, Inc. All rights reserved.

About ThinkHR

ThinkHR provides expert HR knowledge solutions designed to help people and companies thrive. Combining the best of human expertise and innovative technology, ThinkHR’s solutions include the industry’s first and most used HR hotline, an award-winning online HR knowledge base, and a comprehensive eLearning platform.

ThinkHR’s mission is to give its partners a powerful competitive advantage to help them strengthen their client relationships, manage risk and win more business. Equally important, the company is passionate about empowering HR professionals and other executives to become more efficient, productive and successful.

For more information, visit thinkhr.com

ThinkHR
855.271.1050
contact@thinkhr.com

This document is offered for general best practice information only. It does not provide, and is not intended to provide, legal advice.