EBOOK

An Employee Guide to Cybersecurity

Important Tips and Tactics

PEGAS
TECHNOLOGY SOLUTIONS LLC

This Guide provides helpful tips and tactics you can share you're your employees. However, for complete protection you should partner with a Managed Service Provider (MSP) for ongoing, up-to-date Security Awareness Training.

The most dangerous threats to your organization come from the inside – attacks on your employees. By now you know it's essential that you protect your IT network and computer devices. And, of course, that you lock your doors and keep paper documents stored safely.

But, can your employees identify the threats that can get through via email, social media or the Web? Or the physical ones that can come from within, or outside of your office?

The best way to ensure your employees aren't caught unaware is to educate them – and you must do this regularly. Why? Because, criminals constantly change their methods of attack.

Education is the best way to prevent your employees from falling victim to savvy attackers who employ increasingly sophisticated social-engineering methods to gain access to sensitive data.

Social Engineering Threats

Social engineering exploits human behavior to obtain confidential and proprietary information, and to gain access to secure devices and networks. These are carried out when cybercriminals pose as authorities and convince employees to grant access to sensitive data. Social engineering threats are serious and ongoing to the many organizations and their employees who fall victim to these cons.

Phishing emails containing a form of ransomware grew to 97.25% during Q3 2016. This was up from 92% in Q1 2016. There is no one fool-proof way to avoid phishing attacks.

Phishing and Spear-Phishing Emails

This is one of the most-used forms of cybercrime. Criminals use these emails to convince your employees to reveal confidential information (such as bank account and credit card numbers) and credentials (such as usernames and passwords). They pretend to be a trustworthy person, using sophisticated messages to extract this information. They can even pose as your CEO, a business partner, or another employee asking for information.

Phishing. This is when a cybercriminal sends fraudulent communications to your employees. They appear to be legitimate, and claim they're from a trusted source. The employee is tricked into installing malware on their device or sharing personal, financial, or business information.

Email is the most popular mode of communication for phishing attacks, but phishing can be done through chat applications, social media, phone calls, or spoofed websites that are designed to look legitimate.

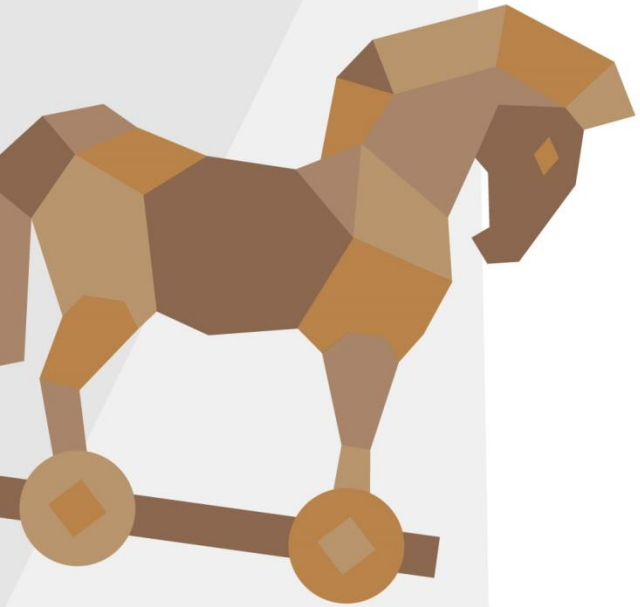
Spear phishing. This is a highly targeted type of phishing attack that focuses on a particular individual or organization. Spear phishing attacks use personal information that's specific to your employee in order gain their trusts. This information can be stolen from the victims' social media accounts or other online activity. Spear phishers have higher success rate for tricking victims into granting access or divulging sensitive information.

In May 2017, the FBI warned that cyber-wire fraud using spoofed email to impersonate a C-level executive or business associate, surged in the last seven months of 2016.

A Phishing or Spear Phishing Email:

- Is one that you didn't initiate.
- May contain strange URLs and email addresses.
- Often uses improper grammar and misspellings.
- Typically contains attachments that you don't recognize as legitimate.
- Contains a link or email address that you don't recognize.
- May use language that is urgent or threatening.

The number of phishing and spear phishing emails are increasing. In addition to CEO cyber-wire fraud, attackers use phishing emails to redirect employees to unsecured websites requesting confidential information, or install Trojans and ransomware via attachments that appear legitimate.



Phishing and Spear Phishing Attacks – Best Practices

Never respond to email solicitations or share confidential information online or over email. Instead, contact the sender directly via phone or with their known email address to see if the message is legitimate. If you receive an email that looks odd from a well-known company, reach out to them using means other than responding to the suspicious email address.

Don't click on links sent in emails. If you must visit a link, type it into your web browser. Don't copy and paste it! Teach your employees that malicious websites can fool them by mimicking legitimate websites.

Beware of Baiting. Similar to phishing, baiting involves offering something enticing in exchange for private data. The "bait" comes in many forms, both digital, such as a music or movie download, and physical, such as a malware-infected device like a USB flash drive or CD labeled "Executive Salary Summary Q4 2016" that's left out on a desk for an employee to use. Once the bait is taken, malicious software is delivered directly into the victim's computer.

No Quid Pro Quos. A quid pro quo attack occurs when criminals request private information from someone in exchange for some type of compensation. For instance, an attacker requests login credentials in exchange for a free gift. Remember, if it sounds too good to be true, it probably is.

Be wary of Pretexting. This is when the attacker fabricates false circumstances to compel your employees to provide access to sensitive data or protected systems. A scammer may pretend to be a trusted entity such as a member of your IT department to trick your employee into divulging login credentials or granting computer access.

It's important to always use the latest operating system, software and web browsers.

Practice Smart Web Browsing

When your employees go on the Internet, they can get "tangled" in vast array of threats lurking on website pages. They may be able to detect some, but others are well hidden.

Encrypted sites are the safest ones to visit. You know a website is safe when you see HTTPS in the URL, and the lock icon on your browser. If you suspect a hacker, do a quick search on the Internet for the subject line.

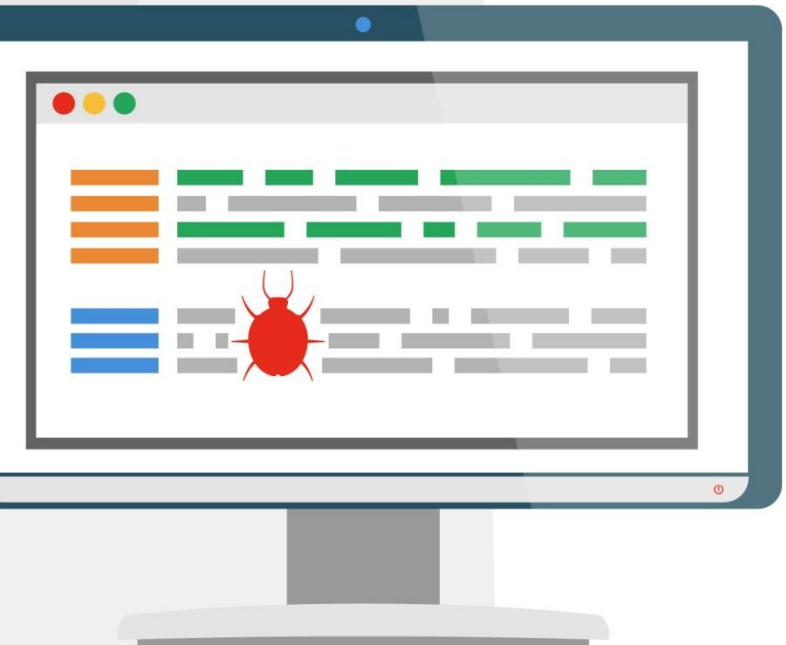
Make sure the site utilizes SSL (Secure Sockets Layer). This a security technology for establishing encrypted links between Web servers and browsers. This is especially important if you're entering your personal or other confidential data into a webform.

Log out of accounts when you're done with them. Simply closing the browser window isn't enough.

Don't link accounts. This allows services to get a lot of your personal information – for example, don't link your Facebook account to other sites when they ask you to.

Consider installing an Anti-Phishing Toolbar. The most popular Internet browsers can be customized to do this. This allows you to check sites you visit and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you. This is another layer of protection you can use, and it's free.

Staying safe when online may seem overwhelming. But remember, everything that connects to the Internet can get hacked.



Watch out for Pop-Ups. Pop-up windows are sometimes phishing attempts. Block them altogether, or only allow them on a case-by-case basis. Don't click on them unless you know they're safe, and don't click on the "cancel" button either – this often leads you to phishing sites. Instead, click the small "x" in the upper corner of the window.

Don't get hooked by Malvertising. This is a form of malicious code that distributes malware via online advertising, hidden within an ad, embedded on a webpage, or bundled with software downloads.

Your browser is the window to the Internet. Browser security is essential to keep your business information safe. A few small tweaks to your employee's browser security settings can make a huge difference.

Safe Web Browsing Settings:

Delete Cookies. Websites use cookies in order to remember your accounts and passwords. They track your web browsing data. Cookies are prime targets for cybercriminals. Delete them.

Get rid of ActiveX. This is an add-on that comes preinstalled on Internet Explorer or Microsoft Edge. It acts as a middle man between your PC and Java/Flash. It can present malicious websites a path into your PC.

Deactivate JavaScript. JavaScript is a programming language to run sites like YouTube or Google Docs. Cybercriminals use JavaScript to infect your devices. Best to disable it.

Don't use browser extensions or add-ons. These pose a security risk – they can open up windows into your PC which can be used to inject malware.

Employee education must be a top priority. Teach them the difference between a strong password and a weak one. And make sure they understand the very real consequences that come from the latter.

Username and Password Management

One of the most common methods everyday hackers exploit are weak passwords. Your employees are probably using some right now.

Use passwords that are easy to remember but hard for others to guess. Think of a phrase like: "I purchased my new car in 2016" and use the initial of each word like this: Ipmnci2017 Use different passwords for each login credential. You can vary them slightly by adding some random letters or numbers. Don't use personal information such as birth dates, pet names and sports teams.

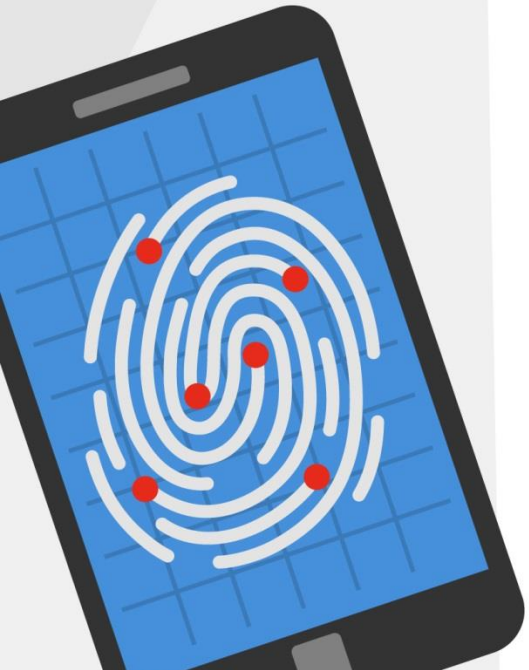
Change your passwords often. Do this at least every three months for non-administrative accounts, and every 45-60 days for admin accounts. You can also use a password manager like Dashlane or Last Pass. These will automatically insert new, difficult-to-crack passwords for you.

Use two-factor authentication. This requires you and your employees to not only enter a password but to also confirm entry with another item like a code texted to a phone.

Don't let browsers save your passwords. While most websites don't store actual passwords, they do store a password hash for each username. Cybercriminals can sometimes use this to reverse engineer the password.

Check online accounts regularly. If you don't, someone else could be using them. Do this for all your accounts, even the ones that you don't use anymore. Have your MSP conduct audits periodically. They can identify weak/ duplicate passwords your employees may be using.

It's essential to not only train your employees in Mobile Security, but to implement Mobile Device Management (MDM) Solutions via your MSP.



Mobile Security & BYOD

If you allow a Bring Your Own Device (BYOD) where employees can connect to your corporate networks through their own devices, then mobile security should be a bit concern. You must protect these, or you open up your business to a huge risk. However, attempting to gain control over personal devices can be a challenge.

What to Watch For:

Hacking. When employees use unsecured public Wi-Fi (in a coffee shop, etc.) criminals in their vicinity can overtake their device without their knowledge. Lost, misplaced or stolen devices. You must be able to remotely wipe a device to protect your sensitive business and your employee's personal data.

Mobile malware. Criminals are executing successful breaches through text messages. Mobile malware can infect both Androids and Apple products. Unsecure third-party apps. If breached, mobile devices can serve as a gateway to your other devices and operating systems, where security controls can be manipulated by criminals.

Sensitive information accidentally emailed to an unauthorized party. Once done, this information is out there forever.

By deploying an MDM platform, you can enforce the use of passcodes to access devices, and locate missing devices. 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.

Tips and Tactics to Protect Mobile Devices

Password-Protect all devices. This means, laptops, phones, smartwatches, tablets and mobile IOT (Internet of Things) devices.

Set a PINs or passcodes. This is your first line of defense. When your devices are password protected it's much more difficult for a criminal to break into them.

Set up Remote-Wipe. Most mobile devices have this capability. Plus, you can supplement them with MDM and the cloud. This way, even if a phone is stolen, information can't be accessed.

Use Remote-Locate solutions. Some software solutions enable you to locate lost or stolen devices through GPS. Apple uses "Find My Phone" and Android the "Android Device Manager." Windows mobile users have this same option from the Windows Phone website. (Consult your MSP on the best ones for your business needs.)

Scan your mobile devices. Smartphones and tablets are essentially little computers. Just like you use antivirus and malware scanners on your desktops and laptops, you should do the same on your phones and tablets.

Security starts at the physical level. All the firewalls, antivirus and other IT precautions in the world won't stop an intruder who can gain physical access to your network and computers.

Physical Security Precautions

Set up surveillance systems. You need a way to know who goes in and out of your facility, and when. Use authentication systems with locking devices, so that a smart card, token, or biometric scan is required to unlock the doors, and a record is made of the identity of each person who enters.

A video surveillance camera placed in key locations is a good idea. They can monitor continuously, or they use motion-detection technology to record only when someone is moving. They can even be set up to send e-mail or cell phone notifications if motion is detected when it shouldn't be (such as after hours).

Protect printers and copiers. Printers and online copiers, like servers and workstations that store important information, should be located in secure locations and bolted down so nobody can walk off with them.

Make sure vulnerable devices are in a locked room. This includes your servers and other network devices. A hacker can plug a laptop into a hub and use sniffer software to capture data traveling across the network.

Physical Precautions for Employees to Abide By:

Beware of Tailgating. Don't let unauthorized individuals who follow you or your employees into your secure location. The goal of tailgating is to obtain valuable property or confidential information. And beware of anyone who wants to borrow your phone or laptop. They can install malware on your device or steal your data.

Make sure to always shred documents before they go into the trash or recycling bin. Criminals will go through your trash to find confidential information. Don't leave mobile phones, laptops, tablets and USB drives out in the open. These often contain sensitive business or personal information.

Turn off computers or put them on lock-down mode when leaving your desk. If you don't, anyone passing by has easy access to all the information on your device.

Never place documents on the desk that contain sensitive information. Keep them locked in drawers and cabinets.

Always erase notes on whiteboards: They may display new ideas/products and proprietary business processes.

Training your employees will heighten their awareness and make them part of the solution rather than a problem.

Store backpacks, briefcases, purses, wallets, keys, security badges etc., safely. Leaving them in the open is an invitation for theft of sensitive information or devices.

Never write user names and passwords on slips of paper or post-its. You can't trust anyone.

Don't display calendars in the open or on computer screens. These may contain sensitive dates and/or information about clients, prospects and/or new products.

This Guide provides helpful tips and tactics you can share you're your employees. However, for complete protection you should partner with a Managed Service Provider (MSP) for ongoing, up-to-date Security Awareness Training.

The most dangerous threats to your organization come from the inside – attacks on your employees. By now you know it's essential that you protect your IT network and computer devices. And, of course, that you lock your doors and keep paper documents stored safely.

But, can your employees identify the threats that can get through via email, social media or the Web? Or the physical ones that can come from within, or outside of your office?

The best way to ensure your employees aren't caught unaware is to educate them – and you must do this regularly. Why? Because, criminals constantly change their methods of attack.

This Guide provides helpful tips and tactics you can share you're your employees. However, for complete protection you should partner with a Managed Service Provider (MSP) for ongoing, up-to-date Security Awareness Training.

The most dangerous threats to your organization come from the inside – attacks on your employees. By now you know it's essential that you protect your IT network and computer devices. And, of course, that you lock your doors and keep paper documents stored safely.

But, can your employees identify the threats that can get through via email, social media or the Web? Or the physical ones that can come from within, or outside of your office?

PEGAS
TECHNOLOGY SOLUTIONS LLC

The best way to ensure your employees aren't caught unaware is to educate them – and you must do this regularly. Why? Because, criminals constantly change their methods of attack.

Contact Pegas Technology Solutions for a complimentary assessment of your IT and cloud computing needs. sales@pegas.io