EBOOK

What You Don't Know Can Hurt Your Kids

PEGAS
TECHNOLOGY SOLUTIONS LLC

Internet crime is the fastest growing crime in the U.S. – And the fastest growing group of victims are children.

Over 45 million children from ages 10 through 17 are online every day. We all know that the Internet can be a great place for them to learn. 95% of schools in the U.S. use the Internet to teach children.

However, it's also a tool for online predators who want to hurt your kids. There are many dangers they can encounter while surfing the Web or hanging out in chat rooms.

Do you supervise your children's Internet use? Many parents don't. Close to 62% of teens say their parents don't know what websites they visit.

When children go online:

- **20%** of them are sexually solicited.
- **25%** encounter unwanted pornography.
- **60%** receive e-mail or instant messages from strangers, and communicate with them.

Over 75% of Internet childhood crimes are sexual solicitations.

Over 100,000 sites involve child pornography.

These Are Just Some of The Dangers Your Children Face.

There are no rules governing the Internet. As a result, your children can visit sites that:

- Detail how to grow and process narcotics.
- Sell stolen products.
- Show how to make fake ID's and make counterfeit money.
- Elicit personal information for illegal purposes.
- Offer "get-rich-quick" schemes that can put you at financial risk.
- Advocate hate, anarchy and terrorism.
- Explain how to make bombs.

71% of parents stop supervising their kids' Internet use after they turn 14.

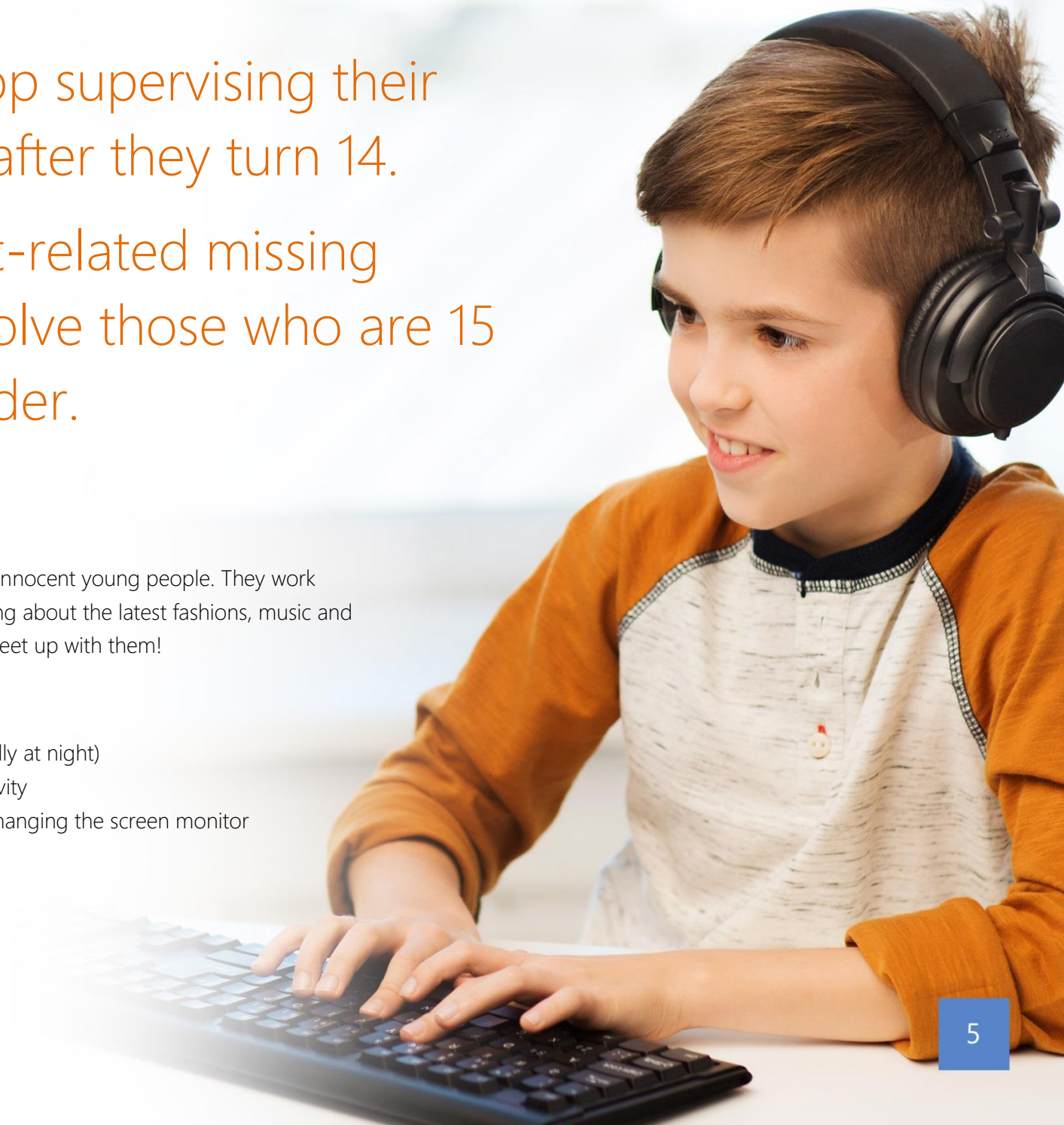
72% of all Internet-related missing children cases involve those who are 15 years of age or older.

Chat rooms are extremely dangerous.

Cyber-molesters are on these sites posing as innocent young people. They work hard to gain your child's confidence by chatting about the latest fashions, music and celebrities, when what they really want is to meet up with them!

What to Watch For:

- Spending a lot of time online (especially at night)
- Being secretive about their online activity
- Quickly turning off the computer or changing the screen monitor when you enter the room
- Changes in behavior
- Unsupervised chat-room use
- Photos of strangers
- Pornographic pictures



If your child goes into online chat rooms, chances are they're talking to strangers. This can lead to private conversations, e-mails, instant messages and photo exchanges that pose great danger to your kids.

They may be convinced to meet with one of these strangers.

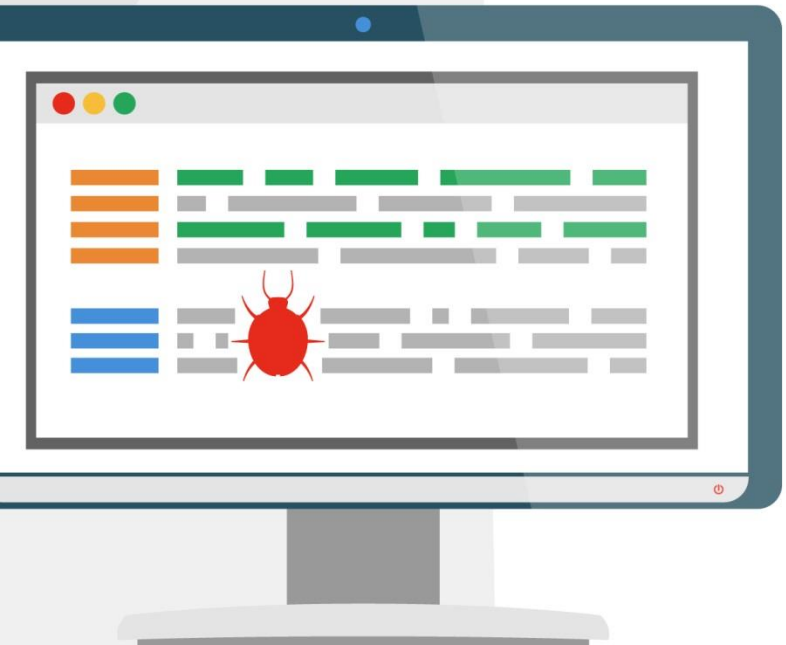
What You and They Don't Know Can Hurt Your Kids.

- Get educated about the Internet and how it can hurt your children.
- Talk to them about the dangers they may face. Spend some time with them online.
- Tell them not to give out any personal information of any kind on the Internet.
- Place their computers in common areas of your home where you can watch them. Supervise their computer use closely.
- Set limits. Don't let them go into chat rooms and don't let them go online at night, alone in their bedrooms.
- Check histories or logs on the computer to see where your children have been.
- Put computer accounts in your name and make sure you you're your kids' passwords.
- Let them know you'll be checking their online activity.
- Use tracking and blocking products on your child's computer. You can purchase these online or in computer stores.
- Use your Internet Service Provider's parental controls and commercial-blocking and filtering tools.
- Have your children sign a pledge to follow certain rules on the Internet.
- If you believe your child is at risk from criminals on the Internet, contact your local police.

ACME CORPORATION

To keep your children safe online, contact {company} in {city}. We can hold an in-service at your place of business to teach you and your staff about the dangers of the Internet, so you can teach and protect your children. {phone} {email}

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.

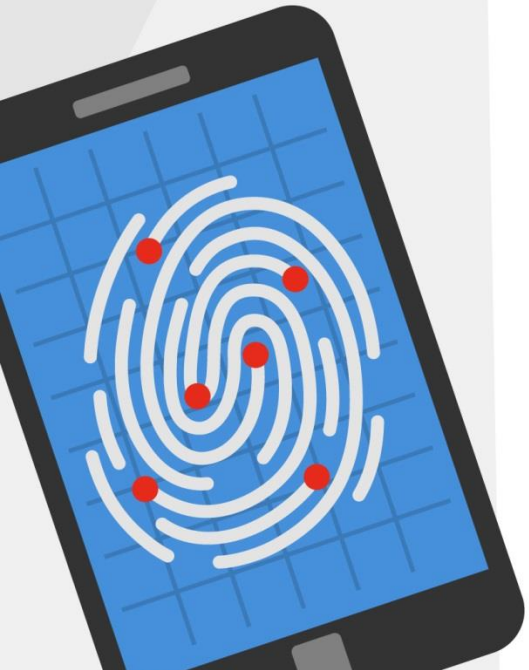
Change your passwords often. Do this at least every three months for non-administrative accounts, and every 45-60 days for admin accounts. You can also use a password manager like Dashlane or Last Pass. These will automatically insert new, difficult-to-crack passwords for you.

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.

However, human error is still highly dangerous, and many employees grow complacent and fail to follow best practices.

Untrained employees are one of the weakest links in your IT defense. That's why ongoing Security Awareness Training is essential.

Depend on Your Trusted MSP to Ensure Employee Cybersecurity

Partnering with a Managed Services Provider (MSP) who has an expertise in IT security can greatly boost your cybersecurity defenses. You need all the most up-to-date tools and solutions to protect against cyber threats.

Your MSP can:

- Keep employee devices updated with the latest antivirus and anti-malware software.
- Apply updates to operating systems, programs and applications – and patches when new ones are released.
- Conduct security assessments to identify weaknesses in your existing IT network and mobile devices.

It's important to have a formalized plan in place to keep security front of mind and employees informed about new threats.

Employee Security Awareness Education isn't just a good idea, it's also required by certain industry regulations and state privacy laws.

Have Your MSP Set Up Ongoing Security Awareness Training.

The cybersecurity training schedule you choose will be dictated by the specific nature of your business and the systems, software and hardware you use. However, a good start would be to ensure all new employees receive training as part of their orientation, and all employees receive training on a bi-annual basis.

Security Awareness Training helps your employees:

- Work with confidence.
- Spot threats before they do any damage.
- Become a part of the security solution rather than a vulnerability.

PEGAS
TECHNOLOGY SOLUTIONS LLC

For more information about this Guide or other Cybersecurity Solutions contact Pegas Technology Solutions at 207-835-4053 or sales@pegas.io