

Feature Stories

Our Partner Eastern Penn Supply

PenTeleData and Eastern Penn Supply partner together to offer reliable connectivity between offices. Read more on this page.

Letter from our GM

Our General Manager keeps us up-to-date on what's in store for the third quarter of 2007. Read what he has to say on page 2.

Phishing, Spamming & Spoofing

Read what they're all about, and how to protect yourself from these ugly predators. Read all about it on page 2.

Is your computer a Criminal?

Do you know what is going on with your computer at all hours of the night? Read more on page 3.

Definition Corner

Get up to speed with definitions that will help you better understand your computer. See page 3.

Customer Contest

Find out what you have a chance to win in this quarter's customer contest, on page 3. Last quarter's winner is on page 4.

To Catch a Con

From bots to scams, Computer Crimes are abundant these days. Read how to fight these computer crimes on page 4.

FUN FACTS

Interesting items and tidbits. . .and you thought you knew everything. See more on page 4.

Partner in Business

PenTeleData and Eastern Penn Supply

Eastern Penn Supply, based in Wilkes-Barre, prides itself on being on the cutting edge of technology. In the 1980s, they were one of the first plumbing, heating and electrical wholesalers in the area to computerize their business.

When the World Wide Web became a viable market conduit, the executives at Eastern Penn Supply, otherwise known as EPSCO, were more than a bit leery. Don Conyngham, Vice President of Sales and Marketing, explains, "We are from Northeast Pennsylvania, after all, where folks will try anything new, as long as Daddy and Grand-Pop try it first. Add to that the fact, this industry for years had signs at the counter saying 'We don't sell to the public' and the stroll into modernity becomes 'climb Mount Everest' in a hurry. Even so, the industry was abuzz with this exciting new media and we all know how CEOs hate to go to the latest convention and not brag up 'we've got that', so we took the plunge."

When asked why they chose PenTeleData over other Internet providers, Conyngham says, "We had no clue about the players, the media, and the challenges. We did get lucky by choosing PenTeleData because they were asking for the business, while others were sitting in offices waiting for us to beg them."

"Today, our computer needs have grown from a dozen 'dumb' terminals and one simplistic main frame to almost a hundred and fifty smart boxes in a virtual network backed by a state-of-the-art server. Data transfer needs have grown with us. We now have T1 lines feeding multiple sites and if there is any delay at all, it's on the operator side, not the service provider. If there is a service interruption, PenTeleData quickly shares with us why it is down, as well as how long it will be down. Whenever possible, they warn us in advance." A T1 from PenTeleData is a high-bandwidth, digital circuit that provides the private point-to-point dedicated connections necessary for fast, reliable Internet and high traffic websites.

With many locations, EPSCO relies on cable modem as a reliable, yet cost effective, means of keeping some of the smaller offices connected. PenTeleData's many options also allow them to utilize DSL and dial-up services where needed.

Internet services have proven successful. This year, Eastern Penn Supply instituted video conferencing training. It has proven to be more cost effective than sending employees to distant training schools. Their web-based business has grown to nearly 2% of all sales, to both contractors and do-it-yourselfers. While that number may seem insignificant, if sales continue to increase at the current rate, they will soon constitute a large part of all their markets.

Conyngham praises PenTeleData's services, mentioning, "To date, PenTeleData is outperforming their promises, which is a good thing! Now if only they could fix the computer network things that make our IT guy go gray – like the employee who when told to 'boot the system' complained, 'it's still not working and now my foot hurts!'"

Maybe they need PenTeleData's Computer Patrol! Computer Patrol offers personalized training sessions, LAN/WAN design, computer diagnostic and repair, wireless networking, software installation and more.

PenTeleData is proud to be an active part of EPSCO's accomplishments. Going forward, we will continue to offer advanced services to meet their growing needs. The only occasional problem we really cannot resolve is the computer asking "Defective user: Replace user? Y/N?"

letter from our General Manager

Dear valued customers,

Welcome to the Summer Edition of our quarterly newsletter, the PTD Chat. This month, in addition to our regular features, you will find some very important security tips for your computer.

First, we'll tell the story of our relationship with Eastern Penn Supply Company, one of the first plumbing, heating and electrical wholesalers in the area to computerize their business.

Then, in our "Definition Corner," we'll explain some of the key words you need to know about the dangers to your computer and your identity.

Next, we share some of the methods used by online predators, including phishing, spamming and spoofing.

You'll also find a brief story about some other online comen, as seen on Dateline NBC.

If you need additional assistance with any of these, consider our Computer Patrol. We'll find you an affordable solution to your security needs.

Last, but certainly not least, enter to win tickets to see the Scranton/Wilkes-Barre Yankees! We're giving a four-pack of tickets for their game against Ottawa on August 27th.

Until next time, have a safe and event-filled summer. We'll chat again in the fall.

Sincerely,
John H. Williams
PenTeleData – General Manager

Phishing, Spamming and Spoofing

With so many Internet threats looming over us, it almost seems like a scare tactic to keep us from using a computer at all. Thankfully, while these threats are real, we can protect ourselves.

Here are some of the Internet thieves' methods, and what you can do to stop them:

Phishing is a method used to obtain personal information, such as user names, passwords, social security numbers and account numbers. Most often, an e-mail explains a problem with one of your bank accounts. The sender asks you to enter personal information, so that they can verify your identity and deal with some urgent issue. What should you do if you receive an e-mail like this?

Attempt to confirm the validity of the message.

You can do this by picking up the telephone and calling your banking institution or by opening up your web browser and typing in the website URL (address) yourself. Do NOT click any links in the questionable e-mail message and do NOT give the sender of the message any personal information about yourself.

Report fraudulent messages and websites. If you confirm the message to be fraudulent, report it to PenTeleData. PenTeleData customers can forward such e-mails and websites to abuse@ptd.net.

Spoofing refers to both e-mail and fake websites. It usually refers to falsifying the true source of an e-mail message or website, in order to deceive the user into believing the message or website is legitimate. Many spam e-mail messages are sent with this intent.

To avoid spoofed websites:

Manually type the address (URL) of a site. Clicking

links in suspicious e-mails may lead you to a spoofed site that looks completely legitimate, but isn't.

Treat all unsolicited e-mails as potential phishing attempts. If you receive an unsolicited e-mail that links you to a website, do not click the links. Treat it as though it is a phishing attempt. Even if the site is not spoofed, some of these sites may install Trojan horse programs or other spyware into your computer that may allow another person access to personal information stored on your computer.

Spyware, also called adware, is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that background information to someone else. Spyware can gather information about e-mail addresses, passwords and credit card numbers.

Not all software that provides ads or tracks your online usage is bad. If you sign up for a free service, you may agree to receive targeted ads and allowing the company to track your online activities to decide which ads to display to you. If you understand and agree to their terms, you may have decided that it is a fair tradeoff.

We have armed you with many helpful suggestions to ward off predators and have taken numerous measures to secure your Internet service, but this threat is serious. **Ultimately, the best way to defend yourself is to secure your computer with virus and spyware protection.**

Upcoming Events

August 3 – 12, 2007

Musikfest

Time: August 3, 5 PM–11 PM
August 4-12, Noon–11 PM
Place: Downtown Historic Bethlehem, Pa.

August 8 – 12, 2007

Carbon County Fair

Time: 3 PM – 11 PM
Place: Palmerton, Pa.

August 26 – Sept. 1, 2007

West End Fair

Time: Sun., Wed. & Sat.,
10 AM – 11 PM
Mon., Tues., Thurs. & Fri.,
Noon – 11 PM
Place: Gilbert, Pa.

August 28-Sept. 3, 2007

The Great Allentown Fair

Time: 8/28, 4 PM – Midnight
8/29–9/2, Noon – Midnight
9/3, Noon – 11 PM
Place: Allentown, Pa

Computer Patrol

Computer Patrol currently serves homes in Carbon, Lackawanna, Lehigh, Luzerne, Monroe, Northampton, and Schuylkill Counties in Pennsylvania and Hunterdon County in New Jersey. If you would like to see Computer Patrol in your area, please e-mail chat@corp.ptd.net. To learn more, visit our website at www.ptdpatrol.com.

If you would like assistance, PenTeleData's Computer Patrol offers professional in-home services, including virus and spyware removal and protection, at an affordable price. Call us today at 1.877.610.9090 or visit our website: www.ptdpatrol.com. We'll come to your home and put YOU in control of your confidential information!

It's 10 PM. Do You Know What Your Computer Is Doing?

The title of this article may make you laugh and think of the commercial, or maybe you are sitting there with a puzzled look on your face. Either way, your computer could be maliciously invading other computers at any time of the day, and you may not even know it.

Bots, otherwise known as zombies or drones, have the ability to silently infiltrate your computer without warning. These attacks infect all types of computers, from residential users to company security administrators – no one is immune.

A bot, in its original form, is not malicious software, and is used in many legitimate ways. Its creators intended them to communicate and control the functionality of Internet Relay Chat channels. Unfortunately, in time, ill-intentioned developers discovered that the bots could be programmed for other automated tasks. Once a computer is infected, you are unlikely to know of

the invasion, or hijacking, because there are usually no symptoms. Groups of these infected computers, known as botnets, can remain dormant and undetected until instructed to perform their next task. This command, controlled by a botmaster, can activate thousands of computers to issue attacks, for sending spam (usually for the intent of phishing), click fraud, identity theft, extortion, spoofing, Denial of Service (DoS) attacks and stock scams.

Criminals, intending to make a profit, can easily lease the bot armies for thousands of dollars a day. Since they often use Internet cafes and other public computers, the identities of these masterminds is difficult or impossible to trace. Their methods have become so advanced that there is no longer a clear distinction between viruses, worms and bots – a new challenge for the Internet community. The epidemic is so large scale that some experts recommend using multiple anti-virus programs. The hope is that if one program misses a virus, another one might catch it.

This problem is very real, and requires a diligent effort to maintain your computer's security. To reduce your chances of becoming a victim, consider these steps:

- > When you are surfing the Internet, beware of the "rough neighborhoods," that is, sites with questionable content. Visiting them can make you more vulnerable to becoming a victim of these crimes. Participating in Internet Relay Chats (chat rooms) can also put you at risk.
- > Never give personal information to an unconfirmed source.
- > Keep your computer's security systems patched.
- > Block unsolicited inbound traffic at your firewall.
- > Run up-to-date virus and spyware protection.

If you would like personal assistance with protecting your computer, consider our Computer Patrol. **We'll use our experience to find an affordable solution for your computer needs. Visit us online at www.ptdpatrol.com or call 1.877.610.9090.**

Definition Corner

When it comes to protecting your computer, knowledge is power. Here are some of the words you should know:

Click Fraud - False clicks on Pay-Per-Click ads to steal money from online advertisers, who pay for each time their advertisement is viewed.

Denial of Service (DoS) Attacks - An effort to prevent a computer resource, such as an Internet site or service, from functioning (often for the purpose of extortion).

Firewall - Security measures designed to prevent unauthorized access to a network or computer system.

Hacker - A computer user who tries to gain unauthorized access to a file or program.

Internet Relay Chat (IRC) - A chat system of large, often worldwide, networks used for communication.

Spam - Unsolicited or undesired bulk e-mail messages, sometimes used to scan a computer's disk drives to gather e-mail addresses.

Spyware - Software that gathers information about a user while he/she navigates the Internet.

Trojan Horse - A computer program that appears to be legitimate, but is intended to perform destructive tasks.

Virus - Software that is capable of reproducing itself to cause harm to other files or programs on a computer.

Worm - A self-replicating computer program that sends copies of itself to other computers to infect or corrupt files.

Software to protect against viruses and spyware is available – don't let your computer be caught without it! For more information, **contact Computer Patrol at 1.877.610.9090 or online at www.ptdpatrol.com.**

Customer Contest - July 2007

PenTeleData is giving one lucky winner a Family 4-Pack of tickets to see the Scranton/Wilkes-Barre Yankees versus the Ottawa Lynx on Saturday, August 27th, 2007.

Rules of the Game:

- Give the correct answer to all three questions listed to the right.
- Then figure out the theme (what they all have in common).

To enter you must answer all three questions to the right and what the theme is between them. Send an e-mail to chat@corp.ptd.net with the following information: your name, address, daytime phone number (where we can contact you), three answers to the questions and the theme. All entries must be received by **8/15/07**.

Good Luck! PenTeleData

Questions:

- 1) Shortly after his inauguration, President James A. Garfield was assassinated by Charles Julius Guiteau on what date in history?
- 2) Wyoming became the 44th state on what date in 1890?
- 3) On what date in history was The Korean War Armistice Agreement signed, ending the Korean War?

To Catch a Con

NBC Dateline's "To Catch a Con" Reveals Lessons for All of Us

From bots to scams, computer crimes are abundant. A recent Dateline NBC two-part series with Chris Hansen revealed the scam behind the e-mails most of us have seen. Desperate characters from distant countries offer a percentage of their claimed wealth for your assistance. You probably just delete these, but thousands of people, in hopes of landing a windfall of money, become victims.

These "419" scams, named for the Nigerian law which makes them illegal, often originate from West Africa. The FBI's John Hambrick participated in the show. He explained that this year alone, at least 10,000 people will be victimized by e-mail cons.

These scams have been around for a few years, but people are still falling for them. In the first of the two-part series, Chris Hansen goes online in search of scammers, and arranges face-to-face meetings. In one case, he uses the name "Jim E. Dimoni", and convinces a supposed government official, "Paul", that he is eager to know more and to invest money. Paul sets up secret codes, faxes "official documentation" and even offers a bonus reward. Jim soon speaks with a "banker", who will close the deal. They meet in London, and Jim is supposed to bring \$14,000 for the "signing ceremony". The week before the trip, Paul asks for a \$3,500 loan to save his family's home. When Jim sends \$200, Paul e-mails that he is "not happy". After tracing Paul's phone

number to a batch of overseas scams, they meet just outside London, in Greenwich. "Anthony", the diplomat, gets right to business, and is in a hurry to get cash from Jim. If he pays, Anthony says that he will release a pile of money that is being stored at the airport, and Jim will get \$3 million for his efforts. Once Jim hesitates, Anthony becomes suspicious, and Jim (Chris Hansen) reveals his identity. Anthony runs off.

With many more scammers to meet, they continue the investigation. After following the trail to others, their face-to-face meetings prove one point - there are several kingpins in these frauds, and they won't be ending anytime soon. Ultimately, if an e-mail promise from a stranger looks too good to be true, it probably is. Just delete it.

In the second part of the series, Dateline proves that anyone with access to your personal information can profit using the Internet. To demonstrate, they worked with a major credit card issuer, and made up names and matched them with real credit card numbers. They offered the numbers to thieves. Within minutes, the crooks began maxing out the cards. The fraudulent charges came from over sixteen different countries, all around the world.

The locations of the conmen, often distant, along with the anonymity of the Internet, allow them protection from law enforcement officials.

According to authorities, it is almost impossible to identify these Internet thieves, so Dateline decided to try. They set up an online store, and advertised it as a "cardable site". This message lets the crooks know that they can use hot (stolen) credit card numbers. While delivering their own packages, they learned just how advanced the schemes can be. Instead of finding the thieves, they found the doorsteps of victims who were manipulated into doing favors for people they met online.

Two of the women thought they were helping a man they met on the Internet. Ironically, both were helping the same person, a man using someone else's picture and calling himself "Paul Desmond". While tracking packages, Dateline also met up with Jeff, who was looking forward to a wedding with "Wendy", a model that he met on the Internet. All three had been accepting packages at their homes, and then sending them to overseas addresses, with the promise of fortune and love. Unfortunately, the packages, shipped with their own money, had been purchased with stolen credit cards. These unsuspecting "helpers" were victims of Internet fraud.

In summary, the Internet is a very valuable tool, but can be used by anyone worldwide. Always be leery of anyone you meet online and never give your personal information or money to unverified sources.

Fun Facts

There are 293 different ways to make change for a dollar.

There are 65 alphabets in use throughout the world.

There are no words in the English language that rhyme with month, orange, silver, or purple.

The word "bookkeeper" is the only word in the English language with three, back-to-back double letter combinations.

Lightning creates glass when it strikes ground containing deposits of sand. Afterwards, streaks of glass fused with the sand can be found.

The most common street name in the United States is Second Street. This is followed by Park Street and Third Street. Main Street doesn't even make the top ten.

The most commonly used language in the world is Chinese. It is spoken by more than 1 billion people.

The most commonly used word in English conversation is "I".

The number 4 is the only number in the English language that has the same number of letters in its name as its meaning.

The number two is the only number greater than zero that, when added to or multiplied by itself, gives the same result: 4.

The only English word with all the vowels in reverse order is "subcontinental".

APRIL 2007 Contest Winner!

Congratulations to Karen Harman of Kreamer, Pa. Karen was the winner of a \$50 Gift Card to Roadies Restaurant and Bar at Penn's Peak in Jim Thorpe, Pa.

- 1) What invasion of World War II, was considered one of the bloodiest battles of the war, and was planned out on April 1, 1945? (Invasion of Okinawa - 1945)
- 2) The launching of the first United States weather satellite marked the first day it became possible to observe the Earth's weather conditions on a regular basis, over most of the world from the vantage point of outer space. What was the satellite's name? (TIROS I - 1960)
- 3) What Emmy Award-Winning drama series hailed by critics as 'The Greatest Soap Opera of All Time', recently celebrated 40 years of broadcasting? (General Hospital - 1963)

Theme: All events that Happened on April 1st