September, 2002

Plus Pages Quarterly

Concepts in Voice and Data Communications

TEL TECH PLUS INCORPORATED

Special Points of Interest

Tel Tech Plus, Inc. Background

Greg Stearns, Chief Operating Officer

Founded in Orange County, California in 1983, Tel Tech Plus, Inc. has since grown significantly as a highly innovative, competitive, and superior performing company providing cost-effective and professionally designed phone, voice mail and data communications systems for business applications, and information technology (IT) services. Currently based in San Diego County, California, Tel Tech Plus, Inc. has multiplied its total revenues several times since incorporating in 1996. This exceptional growth has been due, in part, to our reputation for the highest performance standards and referrals from our satisfied customers.

All our telecommunication and information systems are customized to specific business requirements. In addition to phone and voice mail systems, our scope of expertise encompasses data network cabling, mission critical data center configuration and installation, room set-up for housing telecommunications components, connectivity, and outside plant construction. We maintain a certified RCDD on staff for comprehensive expertise in design and installation. Our general technical staff has extensive experience in installation techniques for numerous types of telecommunication systems suitable for any size business from small offices to large corporate campuses to multiple site locations.

Currently, Tel Tech Plus is engaged in the Navy-Marine Corps Intranet project, which is a $6.9 billion contract managed by EDS to build the largest private intranet in the world. We have installed the structured cabling (i.e., fiber and CAT5E copper) in 12 server farms/data centers, installed cabling to the desktop, engineered outside plant connectivity, assisted with BAN/LAN connectivity, completed IDF surveys and installation, and cutover existing seats to the new NMCI network. Our value-adding efforts and high quality work in shortened timeframes have been applauded across the NMCI enterprise. These attributes are indicative of the work we can do for you and your business.

As a service-oriented provider, our service area extends nationwide. We are known for our prompt response time to service requests and for having a technician available to respond to problems by phone 24-hours a day, 7 days a week.

Tel Tech Plus, Inc. is licensed and bonded by the state of California (#00732562) and is a corporate member of BICSI® and the Better Business Bureau of the San Diego and Imperial Counties. The company is a certified installer for products made by such leading manufacturers as Vodavi, Siecor and Siemon and we support their manufacturer warranties.

This quarterly newsletter is being provided by Tel Tech Plus, Inc. in our continuing effort to keep you better informed about our products and services and items that relate to or affect those products and services.

Inside Future Issues:

IT Information

Phone Systems/ Voice Mail Updates

Company News

Wireless Information

Cabling Updates

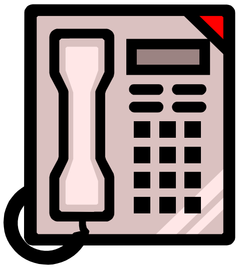
Future Technology Guides

Time is Money:
Remote Programming for Your Telephone System

Randy Quinn, Operations Manager

If you are a believer in the expression that "Time is money" then you are the perfect customer for remote programming of your telephone and voice mail systems. **What is remote programming?** Simply stated, it enables a phone technician to remotely access your phone system and program any feature available on your phone. Additionally, it allows the technician to backup your phone system and voice mail databases.

If you are thinking "Yeah, so what?" then you need to consider the following situation. If your company has high personnel turnover or you require a technician to make program changes quite often, remote programming can save you money. Why pay the cost of an on-site service call for minor program changes when you have an option in the remote programming package to pay a little more than half the price of an on-site service call, and then be billed in half hour increments thereafter? The bottom line is that remote programming can save you almost half the cost of a service call.



Now that you understand the "money" part, let's explore the "time" part of the expression. If you call for a technician to come to your office, that technician will have to be scheduled. There is no guarantee that you will see the technician the same day or even the next day. With remote programming, we can usually have a technician solve a programming problem the same day. You get the work you requested done quicker and at a lower rate than if a technician were to show up on site.

Besides saving you time and money, we can provide you peace of mind through remote programming. We are able to backup your phone system and voice mail databases in the event that you lose them. With the backup, we are able to quickly reinstall the databases and get you and your business in touch with your customers and vendors. This little bit of insurance can make a big difference in your daily business operations.

Are you ready now to consider remote programming? If so, please call our Sales Department today for more information.

Sidebar: Inside the Mind of The Virus Writer and The Hacker

A question often put to me is "Why in the world would anybody want to write a virus or hack a computer?" The motivation of these computer-baddies varies greatly.

In 1988, the Internet came to a near halt after Robert Morris, a first-year Cornell graduate student, released the so-called "Internet worm" into the wild. His intent? To show that users were lazy because they chose easy-to-guess passwords and that server programs were full of holes because programmers did not take security seriously enough. Not so coincidentally, his father was a computer security expert for the U.S. National Security Agency, a major user of the Internet - some said that Morris intended also to "show up" his father in an act of adolescent rebellion.

The Love Bug virus a few years ago appeared in the same way - a graduate student in the Philippines for his thesis project built a program that exploited vulnerabilities in Microsoft Outlook and Outlook Express where Microsoft had blatantly refused to patch the holes. Just like the killer bee, somehow this virus ended up in the wild and in the process, caused billions of dollars in damages around the world. Most of the "proof of concept" viruses have been and will continue to be built with the same purpose in mind - to demonstrate problems in systems, forcing software manufacturers to be responsible and accountable for their poorly designed software and, in the process, twisting the arms of the users of that software to patch their systems.

But those were academic pursuits. Many of the computer attacks are the result of the idle mind being the Devil's playground. There are the Unabomber types - those who have a bone to pick with humanity, multi-national corporations, democracy, American dominance…(the list goes on and on). In their minds, there is no better way to make a statement than by crippling networks or by spraying graffiti across web sites.

Next come the downtrodden - those who feel powerless or disrespected. What if you could be able to build a program that renders systems catatonic, damages files, and/or steals information - all over the globe within an instant - all from one's own home? That, to some, is real power (and in some social circles, brings respect - Machiavelli would be proud).

Finally, there are those out for personal gain: they steal credit card numbers, social security numbers, and other identification information for profit.

Fear not - with proper network and computer design as well as a bit of vigilance, you can stop almost all viruses and hackers cold.

For more information, see the full article in this newsletter on viruses and Trojan horses - the first in a series on computer security by Philip H. Schlesinger.

Defeating Viruses & Trojan Horses

Philip H. Schlesinger, MCSE, CCNA Information Technology Manager

This is the first of many articles on company-wide computer security, explaining the threats to every company's computer systems and how to defend against them.

If you've been using email over the past few years, chances are you've received at least one email with a small but malicious computer program attached. You may have also received a warning that that viruses wandering around computer networks with the hint that you could be next. Klez, PrettyPark, Snow White and The Seven Dwarfs, Mellisa, A Flower For You…the list goes on. Much of this is an attempt to start the fight-or-flight process - in effect to scare people into a sheer panic.

Is the threat real? You bet'cha. But with a small investment in software and the appropriate supervision, your company can bullet-proof itself to stop 99.999% of these malicious programs before they can cause damage.

Malicious computer programs can be divided into two categories:

1) Viruses: programs that seek out and attack systems on their own without human interaction
2) Trojan Horses: programs that require a human action to continue their infective pursuits

Viruses, like their biological counterparts, seek out targets on their own, attempting to break through defenses. Consider them automated hackers, testing the armor that defends computers. If you've ever put a computer directly on the Internet on a high-speed connection such as DSL or Cable (as opposed to behind a firewall - see my next column for more information), chances are if the hackers didn't try to break into your computer, a virus did.

Trojan horses, named after the infamous attack described in ancient Greek lore, are similar to viruses except that they require one thing: the help of a human. They can only cause damage once they are brought through a computer's defenses and then activated by a human. Most of the email viruses of today are Trojan horses: an email shows up, quite often from a trusted individual, requesting that you open an attached file. The attachment's filename may look like a business-related document, a movie, a screensaver, or in the case of the Anna Kournikova Trojan horse, the guise of a nude picture of the tennis star. Open the attached file and you infect your computer.

The damage from viruses and Trojan horses can be huge: files lost, computer systems turned into paperweights, sensitive and confidential data stolen…

Defending against viruses and Trojan horses is easy. Company-wide anti-virus systems have been out for years. A program needs to be installed on every workstation and server to monitor files, web sites, and emails that are accessed. If you have an in-house mail server, you should also have an email scanner running that checks every email that goes in or out. If you have a web or file server accessible from the Internet, even if it is behind a firewall, you should have a program monitoring the traffic to and from the Internet. Once these anti-virus monitoring programs are in place, usually the only additional cost is an annual subscription fee to keep the programs updated with the latest virus definition information so your computers can continue to defend against new viruses and Trojan horses as they are released into the wild.

I mentioned supervision earlier. Once you put these anti-virus systems into place, you need to also make sure that they aren't being bypassed. If given the chance, many people would rather turn off anti-virus programs because they think that the programs slow down their computers (an accurate assessment a few years ago perhaps, but no longer a reality); obviously, if the anti-virus programs are turned off, viruses won't be stopped, so the programs need to be restricted as much as possible and the users need to know that these programs are there for their protection. Computer administrators should also periodically check and make sure that all of the computers are up to date. Finally, I recommend that computer administrators check daily to make sure that the virus definition information is the latest data - sometimes the anti-virus programs will only schedule an update every few days to a week.

About the author

Philip H. Schlesinger has been using computers since the age of 7, when he surprised many people around him by being able to clearly understand the arcane language and syntax used in the DOS 1.0 manual after a single reading. One can only imagine the shock people had in 1981 when he at that age got the original IBM PC to play all kinds of music through its built-in computer speaker using an included DOS program called "samples". Since that day, it has been difficult to pull him away from the keyboard and computer screen for any length of time. He has worked as a computer consultant, systems integrator, project manager, and systems and network administrator - quite often simultaneously taking on several roles. He holds a bachelor degree in Management Information Systems, an associate degree in Accounting, a MCSE (Microsoft Certified Systems Engineer), and a CCNA (Cisco Certified Network Associate). He is also an avid sailor with spinnaker pole duty experience and is an intermediate player of chess. If you are looking for advice on information technology (or need a sailboat racing/cruising crew), you can reach Phil by phone at 760-598-6233 x111 or by email at pschlesinger@teltechplus.com.

On-Hold Messaging

What Do Your Customers Hear When They Call?

. . . do they hear silence, the radio, or music?
On-hold messaging is superior to other alternatives because:

Silence: Callers hanging in silent limbo begin to feel ignored—even 30 seconds wait time seems like forever.

Radio: Licensing fees and fines are expensive and you run the risk of your callers hearing competitors' advertisements.

Music: Licensing fees still apply and it's difficult to select the right music style for all your customers' preferences.

Info-Hold Compact Disc Messaging System is specifically designed to increase your profits. The Info-Hold system includes:

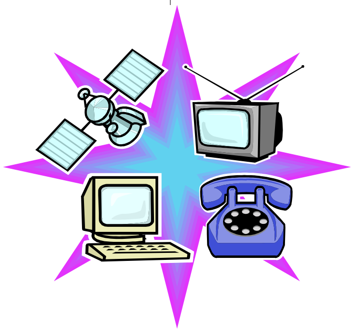
- Protégé CD Messaging Unit—connects to your telephone system and includes an infra-red remote control for easy programming.
- Starter disc Library—8 music tracks, 8 thank you and customer appreciation courtesy tracks, and 8 holiday tracks.
- Customized Message Library—professional copywriters create the scripts for 8 customized messages which are then studio recorded by professional voice talents and set to selected background music.
- Track Legend—rotate and recycle messages by previewing this legend.

Studies show that first impressions influence later buying decisions. The more professional the first impression, the more professional the customer will consider your company to be. Your callers are a captive audience—why not take advantage of the opportunity to promote your business and make this first or second impression really work for you with an on-hold messaging system?

Microsoft Patch Watch

Philip L. Schlesinger
IT Manager

Microsoft issued twenty-eight security bulletins in June, July , and August, 2002, half of which were marked "critical". The big winners were Microsoft's Internet/Intranet system (Internet Information Server, Internet Explorer, Content Management Server, and Internet Security and Authorization Server) with seven patches, followed by SQL Server with six patches. These patches are designed to correct the poor programming designs of various Microsoft software. If your company uses any Microsoft software on your PCs (desktop, laptop, or server), you should check your systems regularly to make sure that they are up-to-date. By installing patches, your company can stop hackers inside and outside the company as well as prevent viruses like Melissa, LoveLetter, MyParty, SirCam, and Nimda from completely taking down your computer systems. Always make sure to have a good backup of a computer before installing patches.



Software patching is one of the many tasks involved with the design, implementation, and maintenance of computer systems. Tel Tech Plus's IT Department can get your computer systems up-to-speed, giving your company the tools it needs to get ahead of your competition.

For more information, contact our IT Manager Phil Schlesinger by phone at 760-598-6233 x111 or by email at pschlesinger@teltechplus.com.