



# information Technology Quarterly

Vol. 5 No. IV

Fourth Quarter 2003

Phil Bertolini, Director, Information Technology

## Paying Traffic Tickets Online

by Mary Gaissert, Application Analyst Programmer - Systems Development and Support

If you are unlucky enough to receive a traffic ticket from one of the four 52<sup>nd</sup> District Courts, cheer up. Now, you will be able to pay the ticket easier and faster than ever before. That's right, on November 17, 2003, a new Web application was launched to allow the public to pay traffic tickets online.

To use the new Web application, just go to Oakland County's Online Services Web page and click the *Pay Tickets* link or go to one of the 52<sup>nd</sup> District Court's Web pages. From the secure *Pay Tickets* site, you will be presented with an instructions page. After reading the instructions, click the Continue button. On the next Web page, enter your last name and the ticket number or your driver's license number. The application will then validate the data and, if valid, display the offense and the fees associated with it. An enhanced access fee for using the Web site will be added to the transaction. If you decide to pay the ticket, you must admit responsibility and enter your credit card information. After a few more clicks, you can print a confirmation page. That's all there is to it!

Time savings will be realized by both the public and the District Court staff when the Web site is used. The public will save time because they will not have to drive to the courthouse and wait in line at the counter. The Court staff will save time by not having to go into the legacy system to mark the ticket as paid as the Web interface does it automatically.

Initially, the system will only allow certain civil infractions to be paid through the Web. If the ticket cannot be paid via the Web, the page will display the offense along with a message "Ticket cannot be paid online". People who see this message will have to follow existing procedures to pay their ticket.

### Inside

<i>Paying Traffic Tickets Online</i> .....	1
<i>Thin Clients Are Coming!</i> .....	2
<i>XP Classes Added To Training Schedule</i> .....	3
<i>Cyber Security: Defense In-depth</i> .....	4
<i>Mouse Break?</i> .....	6
<i>PC Shut Down Procedures</i> .....	7
<i>Computers In The Movies</i> .....	8
<i>Don't Forget To Backup!</i> .....	8

This new application allows for tickets received from one of the four 52<sup>nd</sup> District Courts – Novi, Troy, Rochester and Clarkston. If you receive a ticket from another jurisdiction in Oakland County, you will still have to pay it the old-fashioned way for now. We plan on expanding to all of the Oakland County District Courts in the future.

## **Thin Clients Are Coming!** *by Kevin Bertram, Chief - Technical Systems and Networking*

Phase One of Oakland County's Thin Client project is ready to begin. What is a Thin Client? The answer is simple. A "Thin Client" is an information access device (like a PC) designed to use centralized servers for computing tasks and data storage. All software applications and data reside on central servers and only keystrokes and video are transmitted to and from the Thin Client device. During Phase One of our Thin Client project, selected desktop PCs will be converted to work off central servers located at the Department of Information Technology (IT).

How does an existing PC transform into a Thin Client? Good question! Most County employees currently using desktop PCs have network access to a mainframe, use Internet Explorer to access the Web, have Adobe Acrobat Reader, or use one or all of the Microsoft Suite of products: Word, Excel, PowerPoint, Outlook, or Access. Instead of the majority of this software being located on your PC, it will be removed, utilizing a copy located on a central server. Thin Client users will be accessing a server "farm" which will have multiple network servers to run on in the event a single server is down. Although there is a remote possibility that all Thin Client servers could be down, Mainframe and Internet access would still be possible. Personal data residing on the user's PC will also be moved and located to a central server, again making the PC "thinner". "Heavy" high-failure peripherals such as floppy disks will no longer be used and will be replaced with "lighter" alternative storage devices such as USB Memory Sticks. Last, but far from least, is the heavy financial burden that will be lifted. A Thin Client means a lean and mean budget. Research shows that the average cost of installing, running and maintaining a Thin Client device may be a third of the cost of operating the standard personal computer. Phase One of the Thin Client project is estimated to avoid replacement costs of over \$600,000.

Desktop PCs in the County are currently storing, processing and managing the same software on their hard drives, over and over again. Many valuable work files are stored on hard drives instead of network drives – putting them at risk if a PC crashes or is corrupted. Thin Client devices become much lower maintenance because most issues can be resolved at the central server rather than making a site visit to the PC. When performed at the central server, software upgrades can be more timely and much less labor intensive. Once the software is upgraded, all Thin Client users have access immediately.

Phase One of the Thin Client implementation will pilot the program across the County in divisions in which desktop PCs have been identified as those needing upgrades or replacements and use only the aforementioned applications. Approximately 285 desktops will be replaced with converted PCs that connect directly to servers which will manage all the daily tasks of PC computing. That's Thin Client!

End-users will receive a replacement flat screen monitor, new keyboard and mouse, an upgrade to Microsoft Office XP application software and a different looking login screen. Much like today, users will see application icons in a small window that they will click to launch the programs.

The benefits to Thin Clients are many. In addition to more effectively using IT resources, Thin Clients are more secure, reduce power consumption, are less expensive to replace, streamline customer service, and are more reliable. For more information, visit the Oakland County Thin Client project Web site at <http://www.co.oakland.mi.us/intranet/thinclientpilot> (see the link on the Intranet Start Page) or contact your IT representative.

## XP Classes Added To Training Schedule

Information Technology (IT) is proud to announce the addition of the Microsoft 2002 (Office XP) Suite to the training schedule. To ensure your success, only users who have XP installed on their PCs should register. Similarly, the Office XP courses would also apply to all Thin Client users. Listed below are the new courses to be offered:



**Access 2002 (Office XP): Levels 1, 2, 3, 4**  
**Access 97 to Access 2002 (XP): New Features**

**Excel 2002 (Office XP): Levels 1, 2, 3**  
**Excel 97 to Excel 2002 (XP): New Features**

**Word 2002 (Office XP): Levels 1, 2, 3**  
**Word 97 to Word 2002 (XP): New Features**

**PowerPoint 2002 (XP): Levels 1, 2**  
**PowerPoint 97 to PowerPoint 2002 (XP): New Features**

**Outlook 2002 (XP): Level 1**

**Internet Explorer 6.0: Introduction**

**Windows XP Professional: Level 1**

Each course contains several lessons. Each lesson covers one broad topic or set of related topics. The lessons are arranged in order of increasing proficiency; skills acquired in one lesson are used and developed in subsequent lessons. Notice the "New Features" classes for Access, Excel, Word and PowerPoint. The differences between Office 97 and Office XP will be covered in these new classes.

Did you know that the IT Training Center also provides training to Oakland County cities, villages and townships (CVTs)? This includes the treasurer/assessor offices and police/fire departments. If you know of a CVT employee that needs software training, feel free to refer them to Oakland County.

During the 1st Quarter 2004, only the Introductory and New Feature classes will be offered. Subsequently, the Intermediate and Advanced courses will be added to the next quarterly class schedule. Information Technology will continue to offer the Microsoft Office 97 Suite as well. The training schedule is available for your review under <http://www.co.oakland.mi.us/ittrain/assets/docs/schedule.pdf>. If you have questions regarding the new Microsoft 2002 (XP) or Office 97 courses, contact the Information Technology Reception Desk at (248) 858-0810 or Vickie Worrell at (248) 858-4082.

# Cyber Security

*“A Quarterly Column focusing on education and trends in computer security.”*

## Defense In-depth

*by Romel Rausa Llarena, Data Security Specialist - Technical Systems and Networking*

This past August and September 2003 were tough months for cyber security experts. A multi-state power outage was sandwiched between two highly virulent strains of Internet worms. Fortunately, the County was prepared.

In the cyber security world, this type of preparation is also known as security “Defense In-depth”. Defense In-depth means having security components such as hardware, people, antivirus, firewalls, and policy that are layered and pervasive. Defense In-depth is also about compartmentalizing, isolating, and containing attacks to limit damage.

For example, at the physical level, the Department of Information Technology’s data and communications processing capabilities rely on electricity. Without electricity, the department is unable to operate. As a precaution for such outages, all production systems are connected to uninterruptible power supplies (UPS) that can provide at least half an hour’s worth of production time in the event of a power outage. In terms of Defense In-depth, outages longer than one hour are covered by a diesel generator capable of running the production systems for as long as the generator has fuel. The Defense In-depth covers short-term losses of power as well as long-term loss.

Internet borne worms and viruses are another challenge. At one time, practicing “safe computing” meant running a computer department, for the most part, worm and virus free. Prior to networking, if a machine was infected, another machine could only be infected in the event that media such as a floppy disk was transferred from the infected PC to the uninfected PC. Likewise, when network-

ing personal computers and workstations was still a fairly new concept, an outage rarely impacted getting the work done as networked workstations were not as critical as they are today.

With the advent of the Internet, who could get their work done without a network or even Internet connection? With this dependence on the network along with the large number of machines connected to it (the Internet basically being a large network), comes tremendous exposure to Internet worms and computer viruses. Suddenly the security dynamic and Defense In-depth strategy dramatically changes.

### Technical Terms

**Firewall:** A firewall is a set of related programs, acting as a gatekeeper, that protects the resources of a private network from users from other networks.

**Internet Virus:** A computer program that can reproduce by changing other programs to include a copy of itself. It is a parasite program, needing another program to survive.

**Internet Worm:** Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.


### DICTIONARY



*Cont'd on next page*

The County's current Defense In-depth strategy relies on several components: a firewall at the perimeter, segregation of networks, antivirus checking incoming and outgoing emails, antivirus at the desktop and server, and end-user education and support. The County has several firewalls wedged between the County network(s) and the outside world. Only traffic that is approved by County policy and enforced by the firewall is allowed through. Firewalls are not capable of detecting intent, and it is becoming more and more common for exploits (such as viruses and worms) to pass through a firewall by pretending to be something legitimate when, in fact, it is not (i.e. a legitimate email but with a worm or virus). In such events, the County relies on segregated networks to compartmentalize infections, and antivirus software on workstations and servers to help stave off infections. This layered approach provides an effective defense yet is flexible enough in the event that any of the layers are breached.

**Headlines**



**--Blaster Infected Unprotected PC Within Minutes**  
(13 August 2003)  
In an effort to gauge how fast computers were becoming infected with Blaster, a security company put an "unprotected" PC on the Internet. At one point, the machine became infected in 5 1/2 minutes; later in the day, it took only 27 seconds.

**--Blaster Hits Scandinavian Bank**  
(15 August 2003)  
Blaster wormed its way into servers at all 440 offices of Scandinavia's Nordea Bank; the bank was forced to close at least 70 of its branches in Finland.

Cyber security and Defense In-depth is no longer about just protecting what is the County's. We, as Internet users, owe each other the responsibility of keeping our workstations both at work and home secure and virus free. At a minimum, all workstations today must run some flavor of reputable antivirus software as well as keeping that antivirus software up-to-date.

Keeping up with operating system patches is a must. Patches for an organization like the County takes time to rollout, but for the vast majority of home users, patching has little effect on the workstation and typically is only a few clicks away. Otherwise, your home workstation can become a launching point for infections and attacks. Such home based attacks could have contributed to Air Canada's check-in nightmare on August 19, 2003 after the Welch/Nachi virus infected its reservations systems, prompting the airline to warn its passengers of delays and cancellations.

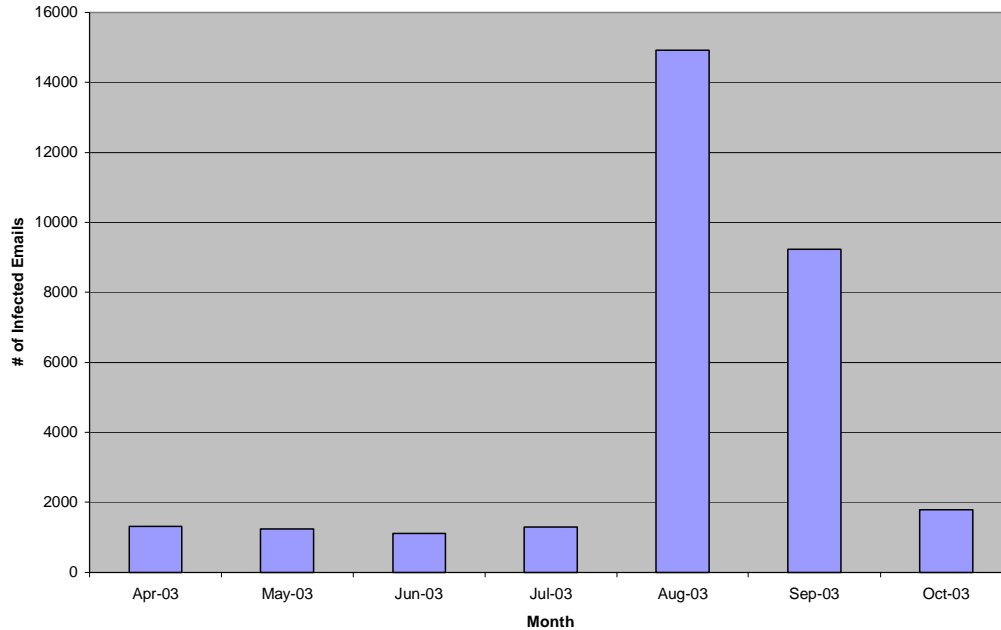
That same day, at the U.S. Department of State, the worm infestation slowed email systems and prompted technical staff to suspend network links between Washington, D.C., foreign embassies and consular offices for nine hours to halt the worm's spread. That move disrupted the Consular Lookout and Support System (CLASS), which is used to check the names of visa applicants against a database containing the names of millions of people who are ineligible to receive a U.S. visa.

The chart on the following page provides information regarding the number of infected emails that have been recently cleaned on the County's email server. Notice the trend in April through July, 2003 followed by a 700% increase in infected emails. Information Technology often performs such tasks as cleaning infected emails in the background...always looking...always detecting...always striving to keep our PCs safe and secure.

Cont'd on page 6

## Trends

Total Infected Emails Cleaned on Email Server in the Past 7 Months



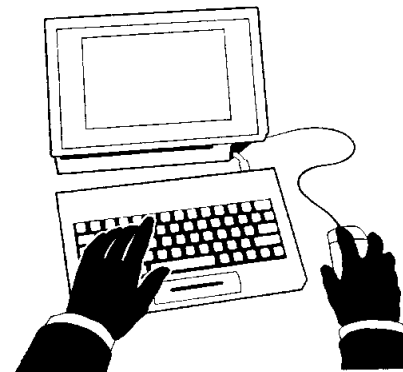
Thanks to Oakland County embracing Defense In-depth, we have contingencies in place to avoid major unexpected service interruptions. If you have questions regarding Internet worms, viruses and/or cyber security, please visit the County home page under <http://co.oakland.mi.us/intranet/virus> or call the Software Help Desk at (248) 858-8812.

---

## Mouse Break?

Almost anything you can do with a mouse you can do faster using key combinations. So maybe it's time you gave the mouse a rest and get to know the keyboard shortcuts. Here are just a few:

- Copy: Ctrl+C
- Cut: Ctrl+X
- Paste: Ctrl+V
- Undo: Ctrl+Z
- Print: Ctrl+P
- Select all: Ctrl+A
- Find text: Ctrl+F
- Go to end of document: Ctrl+End



—adapted from *Computer Shopper*

## PC Shut Down Procedures by Matt Pawlowski, Software Help Desk

Information Technology recommends that you log into the network at the beginning of every day, and log out at the end of every day. Logging in daily is important for several reasons. It is important to refresh your network connections and reconnect to servers that may have been down due to maintenance or other reasons. Also, during the login process you may receive virus definition or other software updates.

While it's a good idea to power down your PC if you will be gone for more than a day or two, powering off nightly is a personal preference. The debate over whether the electricity savings versus machine 'wear and tear' is more important has gone on for years. One thing you should not do is "kill" the power on your machine without logging out properly. This is an unsafe shut down and prevents Windows from properly closing applications, files and connections. If you find that your PC will not shut down properly, please contact the Software Help Desk.

To **log out** of Windows and the network:

- 1) Click the **Start** button (usually located in the lower left corner of your desktop).
- 2) Click **Shut Down**.
- 3) From the **Shut Down Windows** dialog box, click the **Close all programs and log on as a different user** radio button.
- 4) Click the **Yes** button.

This will return you to the **Begin Login** dialog box. This is usually the state you want to leave your PC in at the end of the day. Turn off the monitor to avoid leaving a ghost image on the screen.

Some people lock their workstations overnight by pressing **Ctrl-Alt-Delete** and clicking the **Lock Workstation** button. This is fine when leaving your PC temporarily during the day but it does not log you out of the network. If someone else must use your computer while it is locked, they will have no other option than to kill the power on the machine resulting in an unsafe shut down.

To **shut down** (power off) your computer:

- 1) Click the **Start** button (usually located in the lower left corner of your desktop).
- 2) Click **Shut Down**.
- 3) From the **Shut Down Windows** dialog box, click the **Shut down the computer** radio button.
- 4) Click the **Yes** button.
- 5) Wait for the '**It is now safe to turn off your computer**' message, then press the power button on the PC. It is not necessary to turn the monitor off.

### Important Note for Scheduled Power Outages

Occasionally, Facilities Maintenance and Operations may schedule a power outage at your location for maintenance reasons. It is important that you power down all PCs and other electronic equipment, including monitors, printers, fax machines and copiers. When the power is turned back on, the surge can be too much for a standard surge protector and can cause damage to your equipment. At the end of the day before a power outage, perform the following steps:

*Cont'd on next page*

- 1) **Shut down** your computer. Remember to turn the power off.
- 2) Power off any other equipment plugged into a surge protector.
- 3) Turn off any surge protectors and unplug them from the power outlet.
- 4) Power off and unplug any other equipment not plugged into a surge protector.

These guidelines should cover most situations, however, there are always exceptions. If you have any questions, please contact the Software Help Desk at (248) 858-8812.

## Computers In The Movies

Ever notice that in the movies:

- Word processors never display a cursor.
- Users never have to use the spacebar when they are typing long sentences.
- Users can gain access to any information they want by simply typing: "Access all of the secret files."
- People that type on a computer will turn it off without saving the data.
- A hacker can get into the most sensitive computer network in the world and guess the secret password in two tries.
- Hard drives never crash during key, high-intensity activities. Humans operating computers never make mistakes under stress.



—adapted from *LotsOfJokes.com*

## Don't Forget To Backup!



Whether you have a document saved on a floppy disk, a database saved on your "D" drive, or a spreadsheet saved on a network drive, make sure you have a backup copy, preferably on different media. Equipment fails and accidents happen!

Backup instructions can be found under <http://www.co.oakland.mi.us/ittrain/assets/docs/Winntbu.pdf>. If you have any questions, please contact the Software Help Desk at (248) 858-8812.

### *Information Technology Quarterly*

*Editor:*

*Vickie Worrell*

*Contributing Writers:*

*Kevin Bertram*

*Mary Gaissert*

*Romel Rausa Llarena*

*Matt Pawlowski*

*Published by:*

**Oakland County**

**Department of Information Technology**

1200 North Telegraph Road

Pontiac, Michigan 48341-0421

Phone: (248) 858-0810

© 2003

Visit Oakland County's Home Page at  
[www.co.oakland.mi.us](http://www.co.oakland.mi.us)

*This newsletter is designed to share useful technology news and information with Oakland County Employees!*

*For comments, views, and suggested topics please contact Vickie Worrell at [worrellv@co.oakland.mi.us](mailto:worrellv@co.oakland.mi.us)*