Steps to Computer and Internet Security

Northrop Grumman and Homeland Security Solutions

Strayer University Appoints New President
Consider that almost every computer at our work, school, or home is connected to the Internet and thus exposed to security risks. It is practically impossible to find a computer laptop or desktop without a Web browser, and yet, browsers are the key entry point for many Internet security intrusions. These risks can manifest themselves through email attachments, viruses, worms, and Trojan horses that threaten our networks.

With business operations consisting of a conglomeration of networks, routers, PCs, servers, and software, any Information Technology (IT) weakness leaves the door open for Internet security risks 24 hours a day, seven days a week.

Additionally, the popularity of wireless communication introduces other significant security challenges. Millions of people worldwide are using cell phones, pagers, laptops, and other handheld devices to transfer and store personal and business data. The business environment has shifted away from working within secured settings to working at remote sites if necessary. This has brought about increased risks associated with the transmission of information over untrusted Internet connections, leading to attractive opportunities for third-party access.

One of the greatest risks is exposure to hackers, whose mastery skills allow them to break into computers and access key personal and business information. Hackers can deface Web sites, steal credit card information, exploit server-side scripting, flood the network with bandwidth consumption, and deplete a system’s resources. They can even manipulate routing and DNS tables to point to alternate Web addresses or employ malicious code. Once a system is “hacked” or has been accessed without authorization, all data is vulnerable to illegal or damaging usage.

Although there are many possible risks, there is an equal number of precautions that businesses and individuals can and should employ to reduce outside intrusions. Installing firewalls, updating anti-virus software, and keeping all network systems applications up-to-date are a few steps that can reduce exposure to outside risks. Precautions should also consist of clear and concise implementation plans with continuous assessments of system weaknesses. Furthermore, it is important to provide ongoing education and training for technology personnel as they serve as any system’s most powerful gatekeeper.

As always, users should remain cautious when transmitting personal and confidential information over the Internet. Every computer should be password-protected and, when passing private information via the Internet, be sure to have confidentiality controls in place. These measures can include digital signature, encryption, and digital certificates that facilitate eCommerce transactions.

As the threat of network security has grown, so has Strayer University’s commitment to providing its students with the latest advances in this area. Strayer offers numerous security-based courses that address eCommerce and security, network security, database security, and security design, to name just a few. With increasing employment opportunities in these areas, graduates can expect to find more jobs as software engineers, IT managers, system administrators, database administrators, and information security analysts.

The demand for solid network security education and experience will continue to be strong as threats will surely remain a critical consideration when building and maintaining network systems. The greatest challenge for those responsible for network security will be staying current in the field by regularly seeking education on the latest hardware and software advancements. A highly trained IT team and simple user vigilance can make all the difference in ensuring the security of a network and a risk-free Internet experience. ■

—Pamela Bell
Director, Strayer University Online

User Vigilance: The key to security

With today’s increased security threats, the Department of Homeland Security as well as other government agencies and corporations are placing a high priority on monitoring the Internet for risks in cyber-terrorism, hacking, and state-sponsored information warfare. We cannot take Internet security lightly, but rather, must manage it aggressively.
Features

4 Securing Your System: The Role of the Information Technology Department

6 Steps to Computer and Internet Security

8 Northrop Grumman Corporation Provides Homeland Security Solutions

University News

10 Board of Trustees Names Dr. J. Chris Toe University President

13 Student Satisfaction Survey Results: Students Speak Out on Strayer

14 New Campuses Open in Tennessee

ON THE COVER:
Our cover person, Edwin Khuu, earned a bachelor’s degree in computer networking from Strayer University and is working on his MBA. He is a network manager for the Commodity Futures Trading Commission (CFTC). Edwin recently took some time to share with us some of the security issues we face today and how we can protect ourselves. See the article on page 4 to learn what you should do to ensure your network is secure.

Cover photography by John T. Consoli
As the network manager for the Commodity Futures Trading Commission (CFTC) in Washington, D.C., Edwin Khuu is responsible for the security and maintenance of 60 servers nationwide. He earned his bachelor's degree in computer networking ('01) and is pursuing his MBA at Strayer University.

**How did you become interested in working in Information Technology (IT)?**
When I was 15 years old, I was selected to assist with testing a technology program for Arlington County, Va. At the conclusion of the program, I was recruited by Northern Virginia Community College to be trained for the school's IT support. Soon I found myself advancing in the IT field and expanding my knowledge by working within different facets. Working in these varying areas gave me an understanding of the entire IT network system, which is useful as I move into management roles.

**What are some of the different projects that you are working on at CFTC?**
We have two large-scale projects: our server consolidation effort and the improvement of our Microsoft® Exchange Server. After evaluating several options to complete the server consolidation, we are leaning toward using the combined Storage Area Network (SAN) and clustering solution, where two servers function as one virtual server, and both connect to the SAN. This combined solution provides high availability, reliability, scalability and performance for several reasons. First, our environment continues to operate, while system maintenance is done on one server. Second, the SAN solution allows us to scale up to Tera bytes of data at high performance speed. Whenever a system disaster occurs, one system defaults to the other immediately, and users will not be able to acknowledge a system failure in their data center.

**What are some of the challenges and risks IT departments are facing?**
Implementation of a security plan to keep the network secure (from viruses and hackers) and disaster recovery are daily challenges. In order to implement a security plan to safeguard your network, it is essential to employ the right people. It is important to establish awareness of security issues at every level of an organization, and everybody must be trained properly so they are able to detect and, hopefully, avoid a potential problem. The staff must be able to follow the security plan, communicate and work together to help prevent and solve future problems.

**What should people know in order to protect themselves from unauthorized access both at work and at home?**
There are a few simple steps users can follow to protect their system. First, do not open any files or email attachments that are from an untrusted source. Secondly, it is extremely important to have a unique password to protect your information. A combination of letters and numbers is the best choice to avoid unauthorized use. Thirdly, take time to back up your system and keep the computer’s virus protection software up-to-date.
One of the responsibilities of the IT department is to monitor network traffic. What do you look for when monitoring traffic and what would be considered unusual?

When monitoring traffic, look for patterns. Every corporation’s traffic pattern is different, but there should be some sort of baseline indicating what is normal. For example, if your company typically has high traffic and similar traffic patterns and then, without explanation, the traffic pattern slows down and unfamiliar patterns begin to appear, this is a red flag. In this circumstance, it is necessary to immediately investigate why the traffic has slowed down and where the new traffic pattern originated. Is it application-related or is somebody trying to penetrate your environment? Immediate analysis will indicate the nature of the traffic.

In your line of work, what would you consider a network disaster and how would you recover from it?

A disaster is different for every company based on their needs. While it would be nice to have one uniform disaster recovery plan, every disaster is unique, even for the same company, and thus requires on-the-spot planning. One way companies can prepare is to have a remote server that can pick up where one leaves off if it goes down. This will minimize the down time while the server is repaired. Overall, having a plan for disastrous scenarios coupled with an experienced team is your best chance for a successful recovery.

Are there any federal guidelines and who develops these?

There are no federal guidelines for private corporations, but, as an independent agency of the United States Government, we have National Security Agency (NSA) guidelines we must follow when designing our network security plans. It is necessary for us to work with and report to several different agencies during this process. Due to our affiliation with the United States Government, it is important to communicate the status of our environment. We work with The National Institute of Standards and Technology (NIST), which works to develop and promote measurements, standards and technology to enhance productivity, National Security Agency (NSA), which monitors vulnerability on the Internet, and the Federal Computer Incident Response Center (FedCIRC), which provides assistance with incident prevention and response.

How has your Strayer University education helped your career?

Having worked in the IT field before attending Strayer, I already had technical experience and was looking to gain structured education and theories to advance professionally. The courses I took at Strayer were just what I needed to round out my knowledge and allow me to see the larger picture. While pursuing my MBA, my professors helped me understand how the technical and business sides fit together and how to apply this knowledge to my career as I look to move into management.

What advice would you give to people entering the IT field?

Find your unique area of interest and try everything in the process. It is important to have a general understanding of how the different areas of IT work together and affect each other, but the more specialized you are, the more you can accomplish. Like every profession, it is crucial to find what you enjoy and then stay focused on that area.
There is one simple solution to ensure that your computer network stays 100 percent secure: unplug it from the Internet. Of course, while this strategy may be secure, it is not very practical. Network security is really an oxymoron in the sense that there is no way to ensure that computers stay completely secure. A certain level of risk is always associated with conducting business via the Internet. The good news, however, is that a few simple steps can be implemented to significantly reduce this risk.

One key principle in network security is risk mitigation. Steps must be taken in order to minimize the threat to your computer and network from malicious users or programs. To put this into a better perspective, think of your morning commute to work. Every time you drive a vehicle, there is a level of risk associated with it. Each driver can take steps to mitigate their risk such as fastening a seatbelt, utilizing turn signals, observing the posted speed limit, and staying alert to surrounding traffic. Each precaution further reduces the overall risk of driving a vehicle. With all of these mitigating steps combined together, the risk is acceptable because the benefit received outweighs the risk.

In order to apply this same risk management strategy to our personal computing, we have to take steps to protect ourselves from these threats. A few simple practices will help to alleviate many headaches before they begin:

- **Check security.** Before you submit credit card, financial information, or login data (username and password) online, ensure that the session is secure. This is most easily accomplished in a Web browser by viewing the URL, such as http://www.strayer.edu. A secure http session will be delineated by an “s” that follows the http (https://www.strayer.edu). Some Web browsers will also have another means to identify a secure connection. For example, Microsoft’s Internet Explorer displays a lock icon in the status bar when the connection is secure. This secure connection encrypts the information being exchanged, making it very difficult for a malicious user to get your data.

- **Use personal vigilance.** Never send personal data (credit card, financial information, login data, etc.) via email or chat programs such as MSN® Messenger or AOL Instant Messenger™. Typically these transmission mechanisms do not provide a mechanism for a secure connection.

- **Choose your tool.** Use an anti-virus tool and ensure that virus updates are received at least once a week. There are many commercially available tools on the market such as Norton (http://www.symantec.com) and McAfee (http://www.mcafee.com), but there are also free tools available such as AVG Anti-Virus (http://www.grisoft.com).

- **Build a wall.** A personal firewall helps to ensure that malicious users do not have access to services on your computer. This helps minimize the risk of a hacker gaining access to your computer by exploiting a vulnerable service. Firewalls allow users to specify what traffic can come in and what traffic can go out of their computer and/or network. A firewall is particularly important for broadband (Cable Modem/DSL) users whose connection is high speed.
Chris McDaniels serves as adjunct faculty at Strayer University’s Chesapeake, Va. campus. Mr. McDaniels is also an Information System Security Analyst at Spectrum Comm Inc. located in Hampton, Va.

Firewall solutions are available in both software and hardware/software formats.

The aforementioned steps may seem simple; however, they significantly reduce the risk one may encounter while “plugged in” to the Internet. While it is critical to adhere to these guidelines to help keep your computer network and personal data safe from hackers, it is also important to share this knowledge with friends and colleagues. Malicious users on the Internet will always exist, posing a constant risk. Nevertheless, widespread security education and good security practices will ensure that users have the knowledge to protect themselves from personal data compromise.

Glossary of Terms

**ARPANET** – Advanced Research Projects Agency Network, a pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today’s Internet, and was decommissioned in June 1990.

**Authentication** – Authentication is the process of confirming the correctness of the claimed identity.

**Backdoor** – A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.

**Browser** – A client computer program that can retrieve and display information from servers on the World Wide Web.

**Computer Network** – A collection of host computers together with the sub-network or inter-network through which they can exchange data.

**Cryptography** – Cryptography garbles a message in such a way that anyone who intercepts the message cannot understand it.

**Decryption** – Decryption is the process of transforming an encrypted message into its original plaintext.

**Dictionary Attack** – An attack that tries all of the phrases or words in the dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

**Digital Certificate** – A digital certificate is an electronic “credit card” that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder’s public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

**Digital Envelope** – A digital envelope is an encrypted message with the encrypted session key.

**Digital Signature** – A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn’t changed since transmission.

**Domain Hijacking** – Domain hijacking is an attack by which an attacker takes over a domain by first blocking access to the domain’s DNS server and then putting his own server up in its place.

**Encryption** – Cryptographic transformation of data (called “plaintext”) into a form (called “cipher text”) that conceals the data’s original meaning to prevent it from being known or used.

**Exposure** – A threat action whereby sensitive data is directly released to an unauthorized entity.

**File Transfer Protocol (FTP)** – A TCP/IP protocol specifying the transfer of text or binary files across the network.

**Firewall** – A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

**Internet Protocol (IP)** – The method or protocol by which data is sent from one computer to another on the Internet.

**Intranet** – A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

**Malicious Code** – Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

**Server** – A system entity that provides a service in response to requests from other system entities called clients.

**Virus** – A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—i.e., inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

**Worm** – A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.
GOOD HOMELAND SECURITY IS LIKE GOOD HEALTH: It’s taken for granted and its importance isn’t appreciated until after it’s gone.
Homeland Security (HLS) – A popular term but what is HLS and who makes it work? HLS is a complex activity requiring the synchronized and coherent interaction of the public and private sectors. Given its intricate and critical nature, Secretary Tom Ridge has a daunting task to raise awareness and obtain sufficient funding so meaningful security can be performed. With 14 critical infrastructures (about 95 percent of which have private sector ownership), HLS involves many government organizations, as well as industry, institutions, and citizens who live and work all over the world. The government can pass laws and provide funding, but the vast majority of actions necessary to secure the homeland fall outside of government.

What can be done to achieve HLS? One Chinese proverb could certainly apply: “A thousand-mile journey begins with a single step.” There is no magic bullet or one-time funding to “achieve” HLS. Threats, technology, and the physical domain change, so today’s “fix,” while important to implement and sustain, won’t stop tomorrow’s challenge.

Northrop Grumman Corporation provides HLS solutions to all levels of government, industry, and institutions. The company’s solutions can be found in telephone and computer systems, transportation, law enforcement, intelligence, and defense. This has made Northrop Grumman the number-one provider of security solutions to the Federal government.

Our nation’s way of life is based on our being an open—and trusting—society. We believe people are good and that they will do the right thing. The terrible incidents of Beirut, Dhahran, Oklahoma City, and 9/11 have challenged those beliefs. Not only is our physical security at risk, but so is our cyber security. As a society, we have fully embraced technology for its benefits, but security is often an afterthought. Our computer, landline, and cellular telephone systems—even the supervisory control and data acquisition (SCADA) systems for energy, water, and transportation-critical infrastructures—are at-risk and require risk-mitigating actions.

To begin the journey toward meaningful security, the important first step is to have an enforceable security policy with the full support of leadership. The security policy needs to be based on a realistic and comprehensive security audit. First, threats and vulnerabilities are uncovered and assessed, and then their possible interaction is considered. If a threat is deemed capable of exploiting a vulnerability, then there is a risk. A probability needs to be assigned to this risk so leadership can best determine how to allocate the resources of people, money, and time to mitigate it. Knowing the magnitude of the risk and its possibility of occurring is the basis for determining how much residual risk can be tolerated. This highly generalized process applies to both the physical and cyber domains.

Security isn’t just gates, guards, guns, and dogs. That’s one portion of the physical domain that operates “inside the fence.” But no government, business, or institution is an island. They all have customers and rely on others for services. How will they sustain operations in the face of physical and cyber attacks? Thinking “outside the fence” for power, communications, water, food, and emergency services, as well as taking steps to ensure the extended enterprise of suppliers, customers, financial stakeholders, and others are all viable precautions.

To ensure the United States can continue to enjoy its freedom and liberty, we must all do our part to make Homeland Security a reality.

—by Perry Luzwick, Director, Business Development, Mission Support Systems Defense Enterprise Solutions Northrop Grumman Information Technology
On April 9, 2003, Dr. J. Chris Toe was appointed the 12th President of Strayer University.

“We are very fortunate and pleased to have Dr. Toe as president of Strayer University,” said Scott W. Steffey, chairman of Strayer University board of trustees and chief operating officer for Strayer Education, Inc. “He has a proven track record of success in academics, a strong intellect, and has served as a driving force in maintaining the highest levels of teaching standards.”

In December 2002, the University created a presidential search committee, which included representatives from academia, the board of trustees, Strayer University Online, and University management. The search for a new president began when Dr. Donald R. Stoddard, former Strayer University president, announced his retirement.

“The committee conducted an intensive nationwide search,” said Steffey. “After meeting with numerous candidates, we were convinced that Dr. Toe had the strongest background of academic and leadership experience combined with a solid understanding of Strayer University and its mission. We look forward to his leadership as Strayer University continues to reach adults nationally and internationally in their pursuit of a college education.”

As president of Strayer University, Dr. Toe will serve as chief academic officer and supervise the overall academic direction of the University. Furthermore, he will ensure compliance with the standards of all accrediting and licensing agencies and work with the University’s board of trustees to further the broad vision, mission, and growth of Strayer University. He will also provide guidance and supervision to Strayer University’s regional academic directors and the academic deans.

Dr. Toe joined Strayer University in 1994 as a professor at the Alexandria, Va. campus. During his nine-year tenure with the University, he has held positions of increasing responsibility, including director of graduate programs, campus dean, administrative dean, and academic dean. Since 2001, he has served as the University’s provost and academic dean. As such, he worked closely with the University’s former president to build and solidify the school’s reputation as an institution of high academic quality.

“Through my years at Strayer, I have seen the University grow and broaden its mission,” said Dr. Toe. “We enjoy our reputation as a highly respected institution that is recognized by regional accreditation because of our single-minded focus on quality. My vision is to continue our work as a premier provider of quality, competency-based, post-secondary education while supporting our goal of becoming a nationwide university.”

Dr. Toe earned both his master’s degree and his doctorate in economics from Texas Tech University. A native of Liberia, he earned a bachelor’s degree in economics from the University of Liberia. Prior to joining Strayer University, Dr. Toe served as an associate professor at Texas Tech University. He also worked as an economics consultant in Rome, Italy and Monrovia, Liberia from 1991 to 1993.
An excerpt of the remarks delivered by J. Chris Toe, Ph.D. upon his appointment as President of Strayer University

“As I take the helm of our great 110-year-old institution, I ask each of us to pledge to protect and preserve the academic integrity of our University, and to strive continuously to improve the quality of the education and services we provide our learners. We will maintain our excellent educational reputation, and we will remain a high-quality organization only by assuring our capacity to respond quickly and effectively to changes in the business environment. We will succeed in achieving our institutional mission only by developing and delivering market-driven academic programs, and by providing first-rate support services to our learners.

Strayer University’s best days are tomorrow. The policies, programs, processes and services we initiated have laid the groundwork for institutional growth and prosperity. Our outcomes assessment and information literacy programs, our initiatives in faculty development, faculty selection, and faculty and dean performance evaluation, and our emphasis on academic advising, early registration and other improved support services will assure the success, satisfaction and persistence of our adult learners if we remain responsive, flexible, determined and effective.

We will not attain our high-quality and national expansion milestone without trials and tribulations; we will not execute the opportunities before us without overcoming many challenges. Our organizational culture, which is our greatest strength, must withstand the test of time, new realities, and increased competition; it must also transcend the vestiges of yesterday’s glories and accomplishments if we are to master our future and the challenges of tomorrow.

I believe in teamwork, and I will always strive for common grounds. But teamwork and common grounds are not inconsistent with accountability, responsibility and service. I believe in holding myself accountable and in holding others responsible. I expect all Strayer University faculty to teach and serve, and all campus deans to lead and serve. Every single employee of this University has an obligation to our students, and that is to make their educational experiences at Strayer University equal to or better than our own experiences.

As we return to our desks and other places of work, let us do so not as academicians, admissions officers, or student services staff; let us return as part of a team that will raise this institution to higher elevations. We will succeed in this endeavor only if we resolve to treat our learners as adults, and only if we help learners advance their careers as quickly and as responsibly as possible. Only by respecting our learners and helping them become successful professionals will Strayer University realize its destiny of being a premier adult-focused institution. I ask you to know our vision; I invite you to be a part of our vision; and I urge you to embrace our vision.”
LIBRARY NEWS

Summer 2003

The following resources on network and computer security were located using the Learning Resources Center (LRC) section of the Strayer Web page. Students and faculty have access to these resources via the Web site.

Online Databases

EBSCOHost (Library Web page – Online Databases section: http://studentsserver.strayer.edu/CONT_STD/LIBS/libs2.htm) offers a number of publications covering the subjects of networks and network security. The following provide full-text coverage from the start date listed:

<table>
<thead>
<tr>
<th>Publication</th>
<th>Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Systems Security</td>
<td>Full text from January 1995 to present</td>
</tr>
<tr>
<td>International Journal of Information Security</td>
<td>Full text from August 2001 to present; 12 month embargo</td>
</tr>
<tr>
<td>Journal of Computer Security</td>
<td>Full text from December 1994 to present; 3 month embargo</td>
</tr>
<tr>
<td>Computerworld</td>
<td>Full text from 1999 to present</td>
</tr>
<tr>
<td>InfoWorld</td>
<td>Full text from 1997 to present</td>
</tr>
<tr>
<td>Network World</td>
<td>Full text from January 2002 to present</td>
</tr>
</tbody>
</table>

Online Encyclopedia Britannica offers one article on “Computer Crime” and a number of Internet sites from “The Web’s Best Sites” list:

- Improving Computer Security through Network Design
  http://www.auscert.org.au/Information/Auscert_info/
- Enterprise Security News
  http://enterprisesecurity.symantec.com/content/ESNews.cfm
- IT Security Cookbook
  http://www.boran.com/security/
- Developer Works Security Zone
- Security News
  http://www.securitynews.org/index2.html

Other Libraries

The University of Alabama in Huntsville (UAH), Salmon Library, which is available to students and faculty, offers 37 ebooks under the heading of “computer security.” These can be browsed online for 15 minutes or electronically borrowed for up to four hours. The same search, when extended beyond ebooks, resulted in over 40 hard copy titles that may be borrowed directly.

Other Online Resources – Full-Text Books and Periodicals

The National Academy of Sciences Web site provides over 30 books that are available in full text on the general topic of networks, Internet and security issues:

- Making the Nation Safer: The Role of Science and Technology in Countering Terrorism (2002, 440 pp.)

Strayer University Opens Two Philadelphia-Area Campuses and a Second Raleigh Campus

Strayer University will open two campuses in the Philadelphia region this summer; classes are scheduled to begin September 22. The new campuses will offer all of the Strayer University programs and will also provide access to Strayer University Online courses. In addition, starting in the summer quarter, Strayer will begin offering classes at its new North Raleigh, N.C. campus. Strayer University now has four campuses in North Carolina.

PHILADELPHIA

Delaware County Campus
760 W Sproul Road
Suite 200
Springfield, PA 19064
delco@strayer.edu
1-888-4-STRAYER

Lower Bucks County Campus
3600 Horizon Blvd
Suite 100
Trevose, PA 19053
bucks@strayer.edu
1-888-4-STRAYER

NORTH CAROLINA

North Raleigh Campus
3200 Spring Forest Road
Suite 3214
Raleigh, NC 27616
northraleigh@strayer.edu
919/878-9900
his winter quarter, Strayer University conducted a major survey of its current students to gauge their perceptions of the school and to identify ways to serve their needs better.

A total of 1,528 students participated in Strayer University’s Student Satisfaction Survey. Participants were selected based on a stratified sample of traditional and online courses that polled students from all campuses, degree levels, and academic programs.

Preliminary results regarding students’ educational experience at Strayer University illustrate the reasons students attend the school. Results further show that Strayer University is effective at helping students meet their educational and professional goals through an environment that respects the adult learner.

When asked to rate their overall educational experience at Strayer University, over 90 percent of students indicated that it is good or excellent. This positive evaluation is reflected in the 91 percent of students who would recommend Strayer University to friends and colleagues. By contrast, broad based studies of post secondary education institutions place national averages at only 56 percent in these categories.

The graph below highlights the impact Strayer University is having on helping students meet their educational and professional goals. Over 93 percent of students indicated that Strayer University is having a substantial impact on meeting their educational and professional goals, while 87.9 percent reported a substantial impact on meeting their professional goals.

Additionally, the data shows that Strayer University attends to the concurrent challenges of being a student and working adult. Nine out of ten students agree “Strayer University faculty and staff respect me as an adult learner.” At the same time, 87.5 percent of students agree “faculty members understand the challenges of being a working adult and student.”

The Student Satisfaction Survey will be analyzed extensively to understand students’ needs and to improve how the school serves its students. The preliminary results from the survey show that Strayer University is helping students to meet their educational and professional goals, while providing a respectful and encouraging environment for working adults.

### ALUMNI, STUDENT AND CAMPUS NEWS

#### MARYLAND

**Montgomery Campus**
- Susan Sakmak was selected D.C. Gamma’s Alpha Chi “Outstanding Freshman Honor Student” for the 2002–2003 academic year.
- Cherry Clark was named campus manager.
- Tammy Bird was named campus dean.

**Olney Mills Campus**
- Charlene Avery Ford was named campus manager.
- Oscar Blanco, an International Business student, was awarded the prestigious George M. Booker Collegiate Scholarship.

**White Marsh Campus**
- Kevin Bell was named campus dean.

#### PENNSYLVANIA

**Delaware County Campus**
- Patty Ardoline was named campus manager.

**Lower Bucks County Campus**
- Fatima Arukwe was named campus manager.

#### VIRGINIA

**Arlington Campus**
- Jennifer Holdbrooks Hodge, 2000 MSBA graduate, was promoted to Director of Finance and Strategic Planning at Backus Children’s Hospital in Savannah, Ga.

**Chesapeake Campus**
- Michael Camden, campus manager, will lead a Strayer team of riders in the annual Hampton Roads MS150 Bike Tour this summer to help fight multiple sclerosis.

**Chesterfield Campus**
- James Cox, campus dean, co-wrote a chapter for the book, *The Neurolab Space Lab Mission: Neuroscience Research in Space*, which was recently published by the National Aeronautics and Space Administration (NASA).

#### WASHINGTON D.C.

**Washington Campus**
- The Strayer University chapter of Alpha Chi, the national college honor society, was awarded a Star Chapter Award for 2001–02 at the 2003 national convention.
- Dr. Floyd Tesmer, faculty sponsor of the D.C. Gamma Chapter of Alpha Chi, received the society’s Distinguished Service Award.
- Karen Hardy, 1997 MSBA graduate, was appointed to the Board of Financial Advisors by the Town Council of Atlantic Beach, S.C. Ms. Hardy is founder and CEO of Destiny Capital Funding, LLC, a business finance consulting firm which assists businesses to secure financing for their enterprises.

**Strayer University Regional News**
- Keith Dillon, formerly campus dean at Newport News, was named regional academic dean for the Maryland and Washington, D.C. area.
To celebrate the school’s new Tennessee campuses, Strayer University hosted grand opening events at both the Nashville and Memphis campuses. The event programs consisted of campus tours, keynote addresses on the significance of adult education, and a luncheon for community and business leaders.

In Nashville, Mayor Bill Purcell welcomed Strayer University and discussed the growing demand for an educated workforce. “Educators have long spoken of the need for life-long learning, and this need has never been more urgent than it is today,” said Purcell. “Employers in our state are demanding workers with increasingly technical skills, and this requirement is sending students back to school during many times of their lives. We are pleased to join in welcoming Strayer University to Tennessee to help with this important challenge of preparing our workforce for a new economy.”

Randy Jones, campus manager, Strayer University Memphis, echoed the mayor’s sentiments. “The only thing standing between many of Tennessee’s citizens and career advancement is a bachelor’s or master’s degree,” said Jones. “Our programs are designed specifically for adult students who are working full-time and have family responsibilities. The quality and convenience of our programs are designed to fit the lifestyles of today’s working adults.”

Both of the Tennessee campuses were designed with structural and furniture enhancements along with the latest in computer technology to provide a comfortable and state-of-the-art learning environment.

“We have received an overwhelmingly positive response in Tennessee from students and community leaders,” said Dr. Thomas Risch, campus dean, Strayer University Nashville. “We are looking forward to providing our adult students with the quality, accredited education they need to further their careers.”

Many local businesses were on hand at the opening ceremonies. Autozone, Federal Express, Marriott, St. Jude Hospital and United Parcel Service (UPS) were just a few of the attendees.

“Our new Tennessee campuses will give Strayer University students practical skills they can use in their professions by emphasizing the latest techniques and technologies in business,” said Jim McCoy, Tennessee regional director for Strayer University. “This model has proven successful for many years, and we know it will work for Tennessee.”

Strayer University has built a reputation as a leading post-secondary adult institution that provides quality education with convenience for working professionals. The University has expanded steadily during recent years, adding two to three campuses annually.
Get Your Gear from the Strayer University Gift Shop

ORDER TODAY
Phone: 800-551-6117
703-858-3598
Fax: 703-858-3599
Mail: Meyer Marketing
19535 Newberry Terrace
Suite 207
Leesburg, VA 20176
E-Mail: mmktng@erols.com

You can also fill out an order form online at http://studentserver.strayer.edu, and click on “Virtual Giftshop.”

Please make checks payable to Meyer Marketing.

A. MEN’S IZOD SPORTS SHIRT:
100% cotton knit shirt in stone. Strayer University logo embroidered in burgundy on left chest. Sizes: M – 2XL
Price: $27.00

B. LADIES’ IZOD SPORTS SHIRT:
100% cotton knit shirt in stone with eyelet-tipped collar and cuffs. Strayer University logo embroidered in burgundy on left chest. Sizes: S – 2XL
Price: $28.00

C. MEN’S GOLF SHIRT:
100% cotton, white with burgundy accents on collar and sleeves. Strayer University logo embroidered in burgundy on left chest. Sizes: S – 2XL
Price: $27.00 (add $2.00 for 2XL)

D. LADIES’ SLEEVELESS GOLF SHIRT:
100% cotton, white with burgundy collar. Strayer University logo embroidered in burgundy on left chest. Sizes: S – XL
Price: $25.00

E. DENIM SHIRT:
100% cotton denim long-sleeved button-down shirt in khaki, left chest pocket. Strayer University logo embroidered tone-on-tone above pocket. Sizes: S – 3XL
Price: $30.00 (add $2.00 for 2XL/$4.00 for 3XL)

F. T-SHIRT:
100% cotton heavyweight T-shirt in stone with Strayer University logo imprinted in burgundy on left chest. Sizes: M – 2XL
Price: $15.00 (add $2.00 for 2XL)

G. CREW NECK SWEATSHIRT:
Natural/khaki textured shirt with striped accents. Strayer University logo embroidered tone-on-tone on left chest. Sizes: M – 2XL
Price: $30.00 (add $2.00 for 2XL)

H. BALL CAP:
Two-tone cap in stone with burgundy bill and matching adjustable fabric strap with Velcro closure. Strayer University logo embroidered in burgundy on front of cap. One Size
Price: $15.00

Alumni, Students and Faculty... Send Us Your News

Do you have professional or personal news to share with the Strayer community? Let us know about your achievements (career changes, educational advancements, promotions, and other life experiences). Please provide as much detail and information as possible. Photos are welcome.* Use this form and any extra paper necessary, then mail, fax or email to tell us about yourself.

MAIL Scholar
Strayer University
1100 Wilson Blvd, Suite 2500
Arlington, VA 22209

FAX 703-527-0112

E-MAIL jennifer.freeman@strayer.edu

Strayer University reserves the right to edit all materials used in Scholar.

Name ____________________________________________
Graduation Year ____________________________ Major ____________________________
Campus Attended ____________________________
Address ________________________________________
City __________________________________________ State ____________ Zip ____________
Home Phone ____________________________ Business Phone ____________________________
E-mail ________________________________________ Employer ____________________________
Title ________________________________________
News I’d like to share with the Strayer University community:
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

Thank you for contributing! The submission deadline for the fall issue of Scholar is September 13.
*Photos will not be returned.
Begin your future at any one of these convenient locations.

Over 100 years ago, Strayer University began educating working adults at a single location in Baltimore. Today, we have many more locations but our mission remains the same: provide working adults with the quality education they need to get ahead.

Strayer University's 25 campuses in the mid-Atlantic region, evening and weekend classes, and online courses make achieving your educational goals more convenient. And our quarter system enables you to take more classes in a year than a traditional semester system, so you can earn your undergraduate or graduate degree sooner than you may think. Our next quarter starts June 30. Call now and learn how Strayer University can help you fit education into your life.

We fit your life.

Scholar
Strayer University
2121 15th Street North, Suite 300
Arlington, VA 22201

ADDRESS SERVICE REQUESTED