

Greystone Technology Group, Inc.

THE G:DRIVE

Start the year off right with GT Backup

The data stored on your network is one of your business's most vital assets. The best defense in preventing a catastrophic loss is a solid backup infrastructure including offsite storage of data. GT Backup enables organizations to gain enterprise-class protection for their critical data at a fraction of the cost. GT Backup provides an efficient, reliable and cost effective backup solution with emphasis on security and data retention.

Don't wait until it is too late. Ask your consultant or call us today for more information about our complete solution—GT Backup.

Does your business need a technology tune-up?

Greystone can help. Every client is unique and we make it our business to understand your business. Call us today.



GREYSTONE
Technology Group, Inc.

Hacking into the mind of a hacker

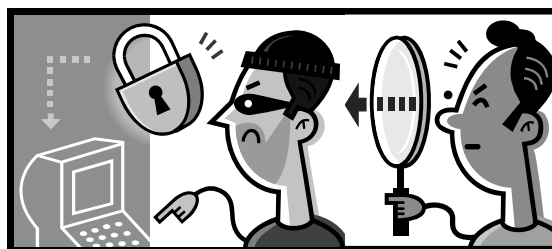
The first thing to know about computer "hackers" is that the term itself is a point of dispute.

Many people who hack into systems without criminal intent proudly label themselves "hackers," and say they're the good guys and the bad guys should be called "crackers" or something else. "Hackers are not evil, malicious people out to damage computer systems and steal passwords. Hackers hate these kind of people," read one e-mail I got after I wrote a column about virus writers.

Others argue that "hackers" represent

both good and bad guys — people who explore and "test" systems for a living or a hobby, as well as those who break into systems to embarrass or rip off companies and people. "Just like in the Wizard of Oz, there can be good witches and bad witches. In the world of hacking, it goes the same way," wrote a reader.

Indeed, all "hackers" aren't criminals. Both good and bad share a common bond and form a highly



caffeinated community where the lines get blurred. At several hacker conventions each year, they talk, among other things, about networks compromised, databases mined, or products where they've found holes. Some are like twenty-something Marc Maiffret, who calls himself "chief hacking officer" at eEye Digital Security in southern California. They begin

hacking networks as naive teenagers, learn the ropes and then put it to use as consultants or corporate security czars.

My purpose with this column is to explore the mindset of people who break into

systems with malicious intent, and then to offer suggestions on how to protect your own system. These people, predominantly males, represent serious threats to the safety of networks and users. Bob Sullivan, a veteran MSNBC.com reporter who's covered the hacker community since 1997, refers to the threatening ones as "computer criminals," "attackers" or "online thugs" — something other than "hacker" to avoid confusion or controversy. I'll follow his lead.

(Continued on page 2)

The contact dilemma — visit, call or e-mail

E-mail has a lot of advantages. You can reach people without having to find them first. You don't have to bother with initial pleasantries, and everyone knows that your brief message doesn't have to be nice. It just has to be factual.

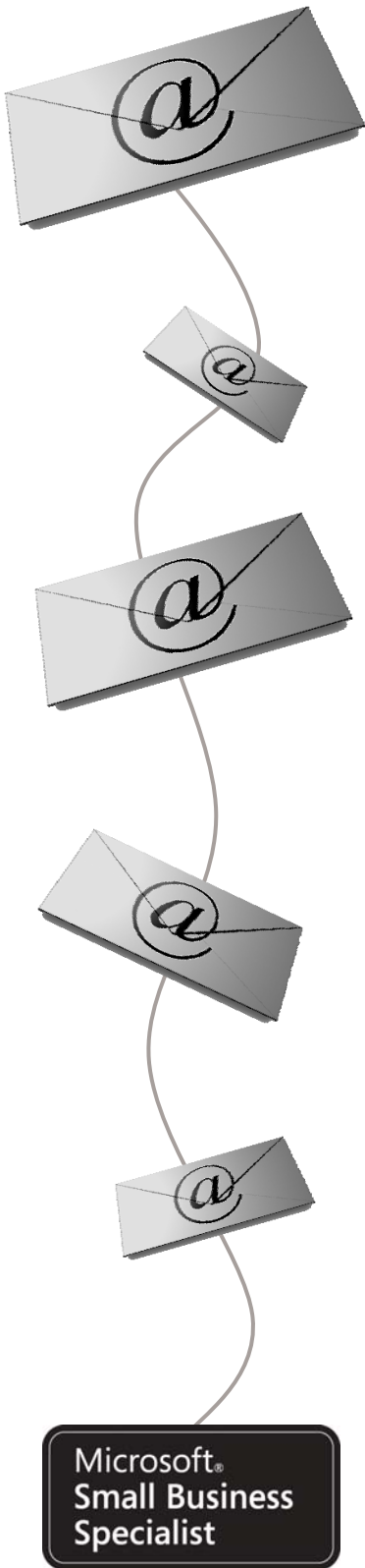
E-mail has taken over business communication in ways that would be better handled face-to-face or over

the phone. How many times have you changed the tenor of what you will say next because of the reaction to your last statement? Would a problem with a customer be handled more quickly if the customer's response was immediate?

The nuance of the spoken voice includes information you would miss with electronic commu-

(Continued on page 3)

Comments? Suggestions? Is there a specific topic you would like us to address? We would love to hear from you. Email Byron Williams at bwilliams@greystonetechnology.com.



Hacking...

(Continued from page 1)

Important things to know about the bad

guys: Hackers in general, and computer criminals in particular, love the power of control. "For many, it's more about the thrill of technology than active malice," says Richard Ford, a security expert and former chief technology officer for Cenetec Ventures. "It's a puzzle to solve, a game to play. For some, it's about money, although these seem to be few and far between." Adds Simson Garfinkel, a computer security researcher and the author of several books on security: "The bad guys want to control as many machines as possible. The majority are in it for fun. They attack the machines of their enemies and of companies. Yet many who break in for fun graduate to breaking in for monetary gain."

They cause the most damage with data theft and fraud.

While technology today is generally becoming more secure, breakdowns are continually exploited and the Internet is ballooning so fast that online thugs have new opportunities EVERY time they boot up. According to statistics from Carnegie Mellon University's CERT Coordination Center, the number of cyber-security incidents — break-ins, virus attacks, etc. — ballooned in 2003 to nearly 138,000, up from 82,000 the previous year. While viruses remain the most common type of cyber-attack, the FBI/Computer Security Institute annual survey in 2003 found those aren't the most damaging. The 530 survey respondents reported a total annual loss of \$70.1 million due to theft of proprietary data, and \$65.6 million due to denial of service, compared to \$27.3 million from viruses.

Any business with a Web site is a target.

Many of today's online thugs use scanners to track unprotected Web sites and networks to attack, says Garfinkel, co-author of "Web Security, Privacy and Commerce." Some can scan hundreds or thousands of sites in a matter of seconds. Garfinkel's own site is protected by a firewall that can track how many times it has been scanned by potential intruders. One particular day, he counted 289,000 different scans, including 1,044 by the same would-be attacker. "Once they find a vulnerable site, they set



up their attack tools," he says. Adds eEye's Maifret: "Know that you could be a target. It doesn't matter what business you are in."

Attackers will get bolder — with blended threats?

That's the fear of Sarah Gordon, senior research fellow at Symantec's security response unit and an expert on the psychology of computer criminals. By "blended threats," she means break-ins combined with virus infections and other methods of destruction, all of which could take down companies' networks in a matter of minutes. Ford agrees. "Massive numbers of systems could be compromised, leading to huge, nationwide outages.

Fortunately, we haven't seen this happen. But I do believe it's a matter of when, not if." So much of the software on computers today is similar, he says, so a problem for one computer is likely to be replicated in others. Gordon adds that with mobile phones and other devices connecting networks to the Internet, attackers have more entry points.

So, how can you protect yourself? Here's what the experts say.

1. Have the best security protection you can afford. Companies with sensitive data need to go beyond basics of antivirus and firewall protection and get intrusion-detection systems and, perhaps, software that pinpoints the vulnerabilities of your system and recommends fixes (see www.eeye.com for more information). Never get complacent — criminal hackers thrive on penetrating "secure" systems.
2. Develop your own company's security policy and guidelines. Put it in writing, and make security a companywide effort. Don't let your employees get away with leaking sensitive information — absent-mindedly or otherwise.
3. Invest in your security personnel. They need tools, training, resources and some authority to make decisions. For many small businesses, managed security services by third-party vendors are the best option, Gordon says.

(Continued on page 4)

The contact dilemma...

nication. One major organization has initiated "no-e-mail Fridays" and encourages people to pick up the phone for a conversation on any day of the week or to see others in person.

The company says that within a few months' time, they experienced better problem-solving, better teamwork, and happier customers.

According to New York University's Stern School of Business, as few as half of recipients get the tone or intent of an e-mail. And most people "vastly overestimate" their ability to relay and comprehend messages accurately.

At Syracuse University, they say misinterpretation is highest when the e-mail comes from a boss.

Has e-mail changed today from the information age to the too-much-information age? With 84 billion e-mails sent worldwide each day, you might think it has.

The days of an instant reply to your message are gone. The recipient has 50 or 60 other messages in line before yours, and unless the tag line is fascinating, your message could be deleted along with many others. Or it could be sent to a folder to be reviewed later.

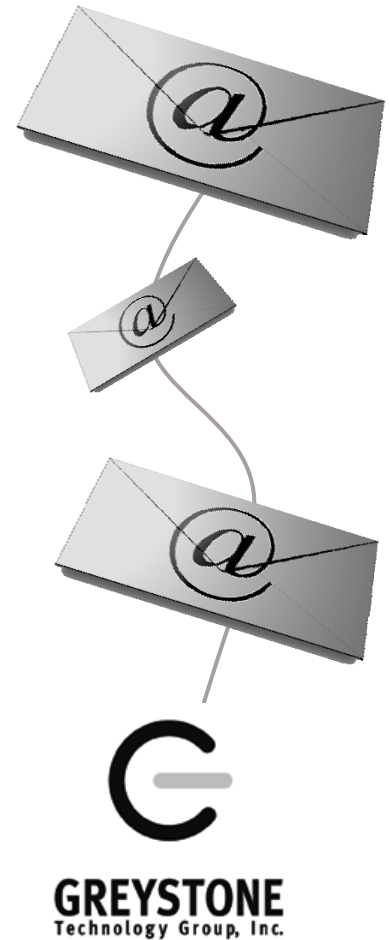
Of course, if you ask two questions in an e-mail, you are likely to get an answer to just one, the question you care about least. One systems administrator says if you ask multiple people a question in an e-mail, often nobody responds.

Phone communications revived. Today, telephones are looking more convenient than ever. When you reach your party, the information you exchange could help you avoid a chain of e-mails.

It's true that you could be directed to voice mail, but once there, the number of calls will be far fewer than the e-mail queue. And the sound of your voice can indicate the importance of the call.

One problem with e-mail is that people love to use it themselves, but they resent it in the hands of CC addicts, joke forwarders, and URL pushers.

The truth? E-mail is here to stay. Sometimes you can save time by seeing a person face-to-face or calling on the phone but you will always run into people who respond to an e-mail much faster due to wireless device abilities. Remember, don't rely on e-mail alone to deliver time sensitive information for you. There can be unexpected delays or delivery issues – e-mail was never intended to become an instant messenger.



11 signs your life is too technical

1. You try to enter your password on the microwave.
2. You consider "mouse elbow" a sports injury.
3. The concept of using real money is becoming foreign to you.
4. You consider 2nd day air delivery painfully slow.
5. The reason you don't keep in touch with some of your family: They don't have e-mail addresses.
6. You chat with a stranger from South Africa, but you haven't spoken to your next door neighbor in more than a year.
7. You consider naming your children "Dot" and "Com."
8. You order take-out food online.
9. You can turn your lights on, open the garage door, turn up your stereo, and see your back yard without leaving your computer.
10. Your idea of a great first date involves a cup of coffee and a chat room.
11. Your dog has an e-mail address.



3801 E. Florida Ave., Suite 630
Denver, CO 80210
p 303.757.0779
f 303.757.0794
www.greystonetech.com



Your referrals are the biggest compliment!

When we provide service for your referral for the second time, your company will receive a two hour credit on your next bill and you will personally receive a \$100 Amazon.com gift card. In addition, your referral's first two hour visit is free of charge. *To refer a potential client, simply fill out our online form at www.greystonetech.com/referral.*

Thank you.

Hacking into...

(Continued from page 2)

- Report computer breaches, and don't cave in to extortion threats. If you are victimized, authorities should be notified, as embarrassing as it may be to you. If you're confronted by an extortionist, don't automatically assume the criminal has all the info he needs to ruin your business. It may be a prankster testing you. "If you aren't intimidated, there may be nothing he can do," says Sullivan, who hears a lot about these pranks. "Bottom line, know your leverage."
- Educate young people on computer morals and ethics. Gordon believes strongly that today's young people need more guidance from parents and teachers on what's right and wrong on a computer. A greater emphasis now may mean fewer computer crimes tomorrow.

By: Monte Enbysk
Reprinted courtesy of Microsoft Corporation

News you can use...

Apple pioneered the all-in-one, single box computer but today PC's have begun making more of the one piece wonders.

Apple's first all-in-one computer that combined a monitor and processing unit came out in 1984. Apple then moved the product up a notch with the popular and colorful iMac in 1998. Today, Apple has one computer which fits into a 7.4 inch aluminum flat-panel monitor case.

PC's evolved along the monitor-and-tower configuration. Their parts generated a lot of heat and required big cases and fans. With new, cooler parts, PC's can now be made in the all-in-one design.

The Gateway One has all of its parts put into its 3.6-inch-thick flat-panel monitor case. It comes with a wireless mouse, keyboard, and remote for \$1,300 to \$1,800. Business Week's Stephen Wildstrom, says he likes the iMac much better.

Sony has launched its Vaio LT PC/TV, which has its parts tucked into a flat-panel monitor that can be hung on the wall.

Hewlett-Packard has updated its TouchSmart PC's to include a touch-activated LCD screen allowing users instant access to the applications they use most.

Quoted in USA Today, tech analyst Roger Kay at Endpoint Technologies Associates says all-in-ones make up only about 2 percent of the worldwide PC market. Wireless technologies make them look nice in a room since they need no cords on the keyboard, mouse, or printer.

Because there's little difference between a flat-panel computer monitor and a flat-panel TV, an all-in-one could serve both purposes in a kitchen or living room.

Why Greystone?

Greystone Technology Group is your in-house IT department dedicated to the success of your business, not just your network. We have a proven track record of creating partnerships with small businesses to make technology work for them. Over the past 5 years we have developed an unmatched level of expertise in serving the unique needs of our customers. Many organizations cannot typically justify the cost a dedicated IT department. Greystone has invested in an expansive set of tools typically only available to large companies. We can use these tools, along with our expertise, to manage, monitor, and protect your system like a Fortune 500 company. Greystone has developed diverse and customizable support models to fit the needs of each of our unique clients. Call or visit us today for more information: 303-757-0779 or www.greystonetech.com.

