tools of the trade

Handy Information and Security

The **Fossil® Wrist PDA** can display the time in nine different analog and digital faces, but it's also a

Fossil Wrist PDA

Palm-powered computer with a high-density 160 × 160 pixel grayscale LCD touch screen with a backlight and stylus that tucks into the watch's buckle. There are buttons on the side of the case for page-up and page-down functions as well as a rocker switch for up/down/enter control. The Palm OS 4.1 drives the Address Book, Date Book, To-Do List, Memo Pad, Calculator, and Time, and it provides support for third-party applications written for the Palm platform. The watch has 8MB of RAM and 4MB of flash memory. The rechargeable lithium-ion battery lasts approximately three to four days, and there's an AC adapter. External synchronization and beaming are achieved by way of USB and infrared ports. You can directly synch up to your PC or beam business cards and other files to Palm devices via the infrared. There are two versions of the wrist PDA—the Fossil and the Abacus—and more information is available at www.fossil.com.

Siber Systems, Inc. has created the **Pass2Go** password management system based on its award-winning RoboForm password and form-filling tool. The application is small, only 3MB, and it becomes completely portable when loaded on a USB thumb drive. It also offers an alternative security for passwords, identities, banking, and credit card information by keeping this kind of information off your PC.

Encrypted on your Pass2Go key, you plug in the access and then remove it without having to store your personal information on the PC. Because it's portable, you can use it on other desktops and laptops, even at Internet cafés, libraries, convention halls, or universities. If the computer has a USB port, your "key" can be used and then removed without leaving the information behind. You can conveniently and safely log on to online accounts or fill in registration and checkout forms by just clicking on your name as it appears in the browser toolbar. You control how much information to include on the forms held on the key, and it's protected with 3-DES encryption. You can download the application from the RoboForm website to add to your USB drive, or it's also available as an OEM product for USB drive manufacturers. Go to www.roboform.com or www.pass2go.com.

Pass2Go Security Drive

It's April 16—Do You Know Where Your Tax Return Is? ◆ Michael Castelluccio, Editor

■ THERE'S SOMETHING PERVERSELY ENTERTAINING about turning the tables on the examiner. When you have been told that a faceless agency has control over whole areas of your life and you don't get to question its rules and procedures, the normal human responses can range from annoyance to paranoia. When that agency is demanding money from you, that's even worse. Add a couple of final absurdities, and you have the IRS. The absurdities? Well, if you call us for a clarification and you happen to be given incorrect information, we apologize in advance, but that's your problem, and any consequent errors remain your fault. Also, please disregard what you might read about so many of the richest organizations in the land paying no taxes—there are just a couple of anomalies in the code you needn't concern yourself with.

So, with a mixed sense of amusement and anger, you might want to download a March 15 memorandum and report of the IRS Audit #200420035 from Pamela J. Gardiner, deputy inspector general for Audit. The subject: "Final Audit Report—While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques" (http://www.treas.gov/tigta/auditreports/2005reports/200520042fr.html). Social engineering? That's what hackers do, right?

continued on next page

The **Nucleus PC Portfolio** from **Pacific Design** is an alternative to lugging your entire briefcase or

Nucleus PC Portfolio

tech bag around once you arrive at your destination. Designed as a "case within a case," the Nucleus Portfolio has room for your laptop, writing paper, and business cards. At 15 × 12 × 2.5 inches, it fits most 15-inch laptops and slides into the computer pocket of other cases in the Evolution line from Pacific Design. Its lightweight (1.75 pounds) molded foam offers a semi-hardshell construction in black or silver, and it has handles and a shoulder strap. Visit www.pacificdesign.com for more details.

Accounting for Practitioners™ release 4 from **Pendock Mallorn, Ltd.**, is an Excel-based trial balance and working paper software used by accountants in companies and public practice. AFP 4 includes automatic lead sheets, grouping schedules, ratio analysis, trend analysis, and complete financial statements that can be customized by the user. An unlimited number of documents can be scanned into AFP, and a user-defined index is created listing each document. Multiple-page documents are numbered automatically. Setup is as easy as entering the company name, address, and fiscal period. Carry forward to the following year is automatic. Journal entry types include adjusting/normal, reclassifying, potential, interim, and tax. Tax entries can be one-sided or balanced. Trial balance views include financial statement, client, prior year(s), and changes from prior year in dollars and percentages. Criteria can be set to flag accounts where the change from the prior year meets the criteria. AFP can import the trial balance as well as up to six journals from any accounting program that can export to Excel. AFP can analyze the journals for amounts equal to, less than, and greater than. Wildcard characters such as * and ? can be used when searching for names. AFP will flag trial balance accounts that have been added, deleted, or changed since the last import. AFP is easy to learn and use, so staff training costs are negligible. The program can be put to use immediately. It has context-sensitive help, and free support is available.
Visit www.pendock/com.

Accounting for Practitioners release 4

continued from p. 55

Progress Has Been Made

In her Ides of March letter, Inspector General Gardiner noted that the agency had "successfully completed significant efforts in securing its computer network perimeters from external cyber threats." But she noted that hackers "are likely to seek other ways to gain access to IRS systems and, ultimately, taxpayer data."

If you were on the outside and wanted to get a peek at the files, or maybe you're an entrepreneur in Eastern Europe and you would like to collect a pile of information including names, addresses, SSNs, banking, credit, and investment information for future use or sale—how would go about it?

Well, you could just ask the agents and supervisors. That's what the Inspector General's contracted testers did. Conning the agents and supervisors—the method is called social engineering—can be done by black hat hackers and investigators of all sorts, good and bad.

The methodology of the test was alarmingly simple. "We placed telephone calls to 100 managers and employees and posed as Information Technology helpdesk personnel seeking assistance to correct a network problem. Under this scenario, we asked the employees to provide their network login name and temporarily change their password to one we suggested."

How do you think they did? Remember, beyond that login name and password stretch carton after carton of returns—out to a distant horizon. Maybe three or four hits out of the hundred, maybe a dozen? "We were able to convince 35 managers and employees to provide us their user account names and change their passwords. Using our test scenario, a hacker or disgruntled employee could obtain user names and passwords to gain unauthorized access to the IRS systems."

With a success rate of one-third, how encouraged do you think a hacker might be? With that kind of payoff at, say, a bank or credit information service, you might expect that hacker to remain in his chair the rest of the afternoon, wandering around the breeched target and looking to transfer everything from funds to credit reports.

This test was conducted after the agency established and posted password rules for its employees. According to Inspector Gardiner, "The IRS requires its managers and employees to acknowledge these rules when they are given access to a system and annually thereafter. In addition, the rules are publicized on the Office of Mission Assurance and Security Services (MA&SS) internal website and during its IRS-wide Computer Security Awareness Week." I guess a few people were out during CSA Week.

If you are wondering how the phrase "progress has been made" became part of the title of this memorandum, you might want to check the Background section of the report. Page 1 includes the following eye-widening paragraph, which explains the encouraging words of the 2005 letter: "In August 2001, with the assistance of a contractor, we conducted social engineering tests on IRS employees as part of our penetration testing efforts. We placed calls to 100 IRS employees, asking them to change their password to one we suggested, and found 71 employees were willing to accommodate our requests." So back in 2001, more than two-thirds were euchred!

Now the door stands only one-third open, which I suppose is a substantial (50%) improvement. But if the slimmer characters quietly slipping in are from Romania and they will be selling the stuff they emptied out of the cartons today to identity thieves in the Philippines tomorrow, things are still way too drafty.

What Were You Thinking?

From the current compromised 35, there were five explanations why they were willing to change their passwords.

1. "They were not aware of social engineering tactics as well as the security requirements to protect their passwords."

2. "They were willing to assist in any way possible once we identified ourselves as the IT helpdesk."

3. "They were having network problems and the call seemed legitimate."

4. "Although they questioned the caller's identity and could not locate the caller's name, which was fictitious, on the IRS' global e-mail address book, they changed their password anyway."

5. "They were hesitant, but their managers gave them approval to assist us."

Obviously, the agency has to schedule another CSA Week. Maybe this time they could hand out big, Day-Glo "Just say no!" stickers for phones and monitors. What bothers me is the question if future lapses that might result in identity thefts will be covered by that agency policy about wrong information—the one that says "We're sorry we misinformed you, but, regrettably, that's your fault"? Will we be hearing, "That's very unfortunate. From Russia, you say. I will ask my supervisor if you can deduct those credit searches you have to do now. Please hold?" ■