Paris' Privates Exposed

The Motley Fool
By Dayana Yochim

Be grateful for Paris Hilton. No, not for filling in where Anna Nicole Smith left off. We have Paris to thank for a timely cyber-security wakeup call. When the contents of her T-Mobile Sidekick — her phonebook, nude photos, and other personal information — were posted on the Internet, entertainment news-watching Americans everywhere were forced to consider the once unthinkable:

If Paris Hilton can get hacked, are any of us safe?

You couldn't be blamed for changing all your account passwords (after briefly toying with the idea of calling the Olsen twins and Ashley Simpson, that is). If nothing else, Paris' plight shows that the effect of cyber invasion can be devastating — even on everyday folk. Well, everyday folk who know Paris. On one technology blog, an alleged T-Mobile service rep reported that a customer whose phone number was in Paris's little black e-book received 2,000 missed calls before he asked to have his number changed.

It is unclear exactly how Paris' bejeweled electronic organizer was compromised — whether T-Mobile's servers, where information is stored, were breached or whether someone accessed her actual device using her password ("Tinkerbell," her Chihuahua's name, perhaps?). The latter is what those in the technology field call an "end user error." Or in non-techie parlance: shooting yourself in the foot.

Whether the security breach was self-inflicted or not, it's clear that as technology advances, so, too, do opportunities for scams. According to a 2004 Federal Trade Commission report on fraud, con artists are increasingly using technology to lure their prey. Internet-related fraud accounted for 53% of all fraud complaints filed last year. Internet auctions (16%), shop-at-home/catalog sales (8%), and the broad Internet services/computer complaints category (6%) topped the list of crimes and misdemeanors.

The leap from fraud to felony isn't hard to make. Sure, buying merchandise that is never delivered is a pain in the keister; and posting someone's contact list and "Cute Outfit Ideas" file on the Web certainly is an invasion of privacy. But even more devastating is identity theft — when a thug uses your vital stats to open a credit card or cell phone account, get a loan or take over a bank account, pass bad checks or commit government benefits fraud in your name. The FTC says that identity theft accounted for 39% of the 635,000 complaints filed in 2004. Other studies estimate there were 7 million to 10 million incidents of identity theft last year.

Continued on back

Given how much information people store on their hard drives and handhelds, it's no wonder ID snatching's on the rise. Just last month, coincidentally, a T-Mobile security breach exposed several hundred customers' information, including the cyber thief's Rosetta stone: Social Security numbers.

Have you been "Hilton"-ed?
Before you trash your Palm Treo and blacklist **Research In Motion's** BlackBerry handhelds, first see whether the bad guys have even come calling. Look for clues in your credit file: Signs of wrongdoing often appear there first. And be sure to review the data with the all three major reporting bureaus, since the information is not collectively shared among them

Paris was lucky: Most victims don't discover what the bad guys are up to for weeks, months, or even years. Hilton and her famous friends knew pretty quickly that something was up when their phones started ringing off the hooks. In no time the FBI, Secret Service, and a team of forensic technicians were on the case. Not-so-famous victims of identity theft spend an average of $500 and — get this — 30 hours to clear their names, and that doesn't include the average loss per victim of nearly $5,000.

Save yourself some headaches and some Benjamins and start taking precautions now, before any of your unflattering photos or private data are posted online.

To guard against cyber crime:

Password-protect everything. Use a complex assortment of nonsensical words, numbers, and random punctuation marks. Once you have your password memorized, it's time to change it. Seriously, though, change your passwords often and share them with no one. If you have a weak short-term memory, record them far from the devices they are protecting.

Don't put the good stuff on a handheld device. If you do lose your PDA or if someone manages to crack your electronic Fort Knox, having your Social Security number, a list of bank and brokerage accounts and a map to those buried gold bars only compounds the potential damage. (If you're a young blonde heiress who's not camera shy, you might also want to consider stashing your revealing photos and videos in an actual vault.)

Don't click that! By now you've probably gotten several hundred notices from banks with whom you do no business telling you there's a problem with your non-existent account. This is called "phishing" (as in "fishing for a sucker to take the bait"), and it can be avoided by simply ignoring the solicitations. But what about the less obvious come-ons? Take a tour of your computer to see whether anyone's lurking. The CERT Coordination Center (operated by Carnegie Mellon University) has a library of Internet security tips — from installing initial security measures to responding to incidents and fixing email abuses. PDAstreet.com has bulletin boards where you can learn about the latest concerns (and cool stuff) for nearly every handheld device.

Continued

Make creditors call you before any funny business occurs. Ask the credit reporting agencies to put a fraud alert on your file. (By calling one, all three will comply.) It requires lenders to request additional documentation from you anytime you request credit. If you get a call about a credit application you didn't fill out, you can stop a thief in his tracks. It will also opt you out of pre-approved offers. Fraud alerts expire, so make a note of when you need to re-up. Here are the contact numbers: Equifax: (888) 766-0008, Experian: (888) 397-3742, TransUnion: (800) 680-7289.

Next, go analog and protect yourself from low-tech criminals:

Thwart the old-fashioned crime of wallet-snatching. Photocopy the contents of your wallet — all cards, back and front. Don't carry important documents, such as your original Social Security card or a passport, unless you need to. Eliminate personal information (such as your Social Security number) from your checks, and ask that it not be the identifier on documents such as your insurance card

Give trash-picking thieves less fodder. Take your name off the junk mail lists. Opt out of pre-approved credit card offers — gold to ID thieves — by calling 888-5OPTOUT (888-567-8688). Buy a cheap shredder, gather any official documents destined for the trash, and pretend you work at Enron during commercial breaks.

Check your bills. No, really. Check them. It's tempting to just glance at a bill and dash off a check. But a small, innocuous mistake may really be a fraudster checking to see whether he's tapped into a usable account. Review your credit card, cell phone, dry cleaning, and other bills for any unusual activity, and don't feel bad about canceling accounts that you think have been sullied.

Look out for Aunt Edna. Many identity thefts are committed by someone close to the victim. That probably shouldn't be as big a surprise as it is: Family members have easy access to all the necessary documents and can keep a close eye on their mark (often, the elderly). Even work acquaintances can poke around your desk after office hours without raising eyebrows. Unfortunately, you can never drop your guard. It may feel weird to narc out someone with the same last name, but shared DNA doesn't give anyone the right to rip off a loved one.

This is, sadly, only a partial list of protective measures. If you're really paranoid, make the FTC's ID theft website your home page. It's regularly updated with the latest scams.

Finally, it bears repeating: Thank you, Paris Hilton. By going public with your pain, you've shone a much-needed light on the importance of keeping one's private parts, well, private.