Hackers Use Two New Tricks
To Steal Online Identities;
Scams Are Harder to Detect

By KEVIN J. DELANEY
Staff Reporter of THE WALL STREET JOURNAL

May 17, 2005; Page B1

Phishing is so 2004. This year's new Web threats are "pharming" and "evil twins."

Many consumers have grown savvy to "phishing" scams, which use fake emails that appear to come from banks or other businesses to con recipients into supplying personal data over the Web. So fraudsters have come up with new tricks to steal identities online that are even harder to detect. Security experts say two of these scams with some of the most damaging potential are called evil twins and pharming.

Evil twins are wireless networks that pretend to offer trusty Wi-Fi connections to the Internet like those available at some coffee shops, hotels and conferences. On a laptop screen, an evil-twin Wi-Fi hotspot can look identical to one of the tens of thousands of legitimate public networks that consumers log on to every day, sometimes even copying the sign-in page. But that's just a front, and fraudsters who set up the connections attempt to capture any passwords or credit-card numbers that consumers using the link may type.

In pharming, thieves redirect a consumer to an imposter Web page even when the individual types the correct address into his browser. They can do this by changing -- or "poisoning" -- some of the address information that Internet service providers store to speed up Web browsing. Some ISPs and companies have a software bug on their computer servers that lets fraudsters hack in and change those addresses.

Pharming and evil twins aren't yet widespread and certainly haven't become the huge problems that phishing and spyware are. But they're insidious because they can be harder to detect. The growth of such scams shows that the cat-and-mouse game between fraudsters and those seeking to safeguard consumers online is far from over.

Evil twins "are the new frontier" in ID theft, warns Ken Silva, chief security officer at Verisign Inc., a Mountain View, Calif. company that provides Internet-security services. Hackers in the past have eavesdropped when consumers use legitimate Wi-Fi services in public places. But consumers have been able to use encrypted connections and other techniques for safeguarding their data.

Now, evil-twin wireless networks can thwart some of those precautions. During a tech conference in London last month, fraudsters set up a Wi-Fi network masquerading alternately as the conference-provided free wireless connection and as networks from BT Group PLC and T-Mobile, a unit of Deutsche Telekom AG. But when unsuspecting users connected, the Wi-Fi service infected their PCs with an array of 45 viruses, including some that gather information on the user, according to AirDefense Inc., a wireless-security company.

Similar evil twins surfaced again at another conference in Las Vegas earlier this month. AirDefense Chief Security Officer Richard Rushing says he spotted seven different evil-twin networks in one day, including another T-Mobile imposter and one pretending to be a Hilton Hotel network. When a user connected to those networks, he saw a Web page that by all appearances looked identical to the legitimate services, including boxes to enter login information. Mr. Rushing believes the fraudsters just copied the original Web page files and served them up from their own computers.

"This issue is not isolated to one company, but the entire industry," says Kyle Warnick, a T-Mobile spokesman in the U.S.

Evil twins don't appear to pose much of a threat to people connecting to Wi-Fi networks from their homes -- hackers are looking for large numbers of people using Wi-Fi, say at an airport lounge. It's also still not clear whether the fraudsters have succeeded in stealing any sensitive information using the technique. Mr. Rushing says he believes that data theft has happened, partly because evil twin networks are so easy to set up, requiring little more than a laptop computer equipped with a Wi-Fi card. With a second Wi-Fi card, hackers can also easily supply real wireless Internet service to unsuspecting users and then comb through data from those people for passwords and other sensitive information. The evil twin tactic "really hasn't been exploited to its full potential," Mr. Rushing says.

To protect themselves, consumers should turn a laptop's Wi-Fi function off when not in use to avoid accidentally connecting to an evil twin, security experts recommend. Some advise users to sign up for Wi-Fi services, such as the T-Mobile networks available in many Starbucks coffee shops, from computers with fixed-line Internet access so they don't have to send credit-card numbers over a wireless connection. T-Mobile provides free connection software for laptops that automatically checks a Wi-Fi network's digital ID certificate to make sure it's legitimate.

Like evil twins, the emerging threat of pharming can easily pass under most computer users' radar. That's because pharming victims type the legitimate address in their Web browsers and end up at phony sites anyway.

The bad guys can exploit a common procedure used by Internet-service providers to offer faster Web service. When someone types, say, "www.citibank.com," the ISP needs to know the Internet protocol address that corresponds to that name, a string of numbers such as 192.193.217.120. ISPs can look up those numbers by contacting special online computers. But many ISPs instead store a list of common Internet protocol addresses so they don't have to do this lookup procedure. The software bug relates to this fact, letting fraudsters hack into the list using a technique known as "DNS cache poisoning." Variations of the bug have been around for years, and fixes are available. Still, an estimated few thousand ISPs and companies that haven't gotten around to patching the bugs were affected in a recent attack.

Security experts say the problem isn't going away. "One would think there's an easy solution, but there's not," says Johannes Ullrich, chief research officer at the SANS Institute, a computer-security research and training organization in Bethesda, Md.

In one case that began in March, hackers used a computer in South Korea to exploit the flaw and substitute phony IP addresses for real ones on servers used by thousands of organizations, including companies and ISPs. Individuals at those organizations attempting to access American Express Co.'s Americanexpress.com, Citigroup's Citicards.com, Microsoft Corp.'s MSN.com and hundreds of other sites were directed to Web pages set up by the hackers, according to SANS's Internet Storm Center monitoring service. Those other Web pages tried to install spyware on users computers that could watch what users did online and gather information about their PCs. The hackers eventually succeeded in rerouting attempts to reach any Web address ending in ".com" from any of the affected organizations.

While nefarious, these attacks didn't route users to Web sites resembling those of legitimate organizations, such as banks. But security experts warn that they demonstrated the risk of any future attacks that did so.

One way for consumers to protect themselves is to make sure they land on special secure Web pages that use encryption to protect data transfer, a standard practice for any financial Web site. Behind the scenes, those sites automatically present users' browsers with digital ID certificates to verify their legitimacy -- and browsers warn users if the certificates don't match up. The Web addresses for such secure pages begin with "https" rather than the standard "http."

Even with such precautions, security experts acknowledge that pharming and other budding ID theft threats are especially challenging to counter. "All of the burden rests with the user, who's probably the least able to fix these things or recognize them," says Mr. Ullrich.

--David Bank contributed to this article.

Write to Kevin J. Delaney at kevin.delaney@wsj.com