Gartner

Research

Publication Date: 22 June 2005 **ID Number: G00129146**

Increased Phishing and Online Attacks Cause Dip in Consumer Confidence

Avivah Litan

The number of phishing attack e-mail recipients grew 28 percent this year, according to a new Gartner survey of 5,000 online U.S. consumers. These and other breaches are exacting a steep toll on consumer confidence and will inhibit three-year U.S. e-commerce growth rates by 1 percent to 3 percent.

WHAT YOU NEED TO KNOW

Phishing and other cyberattacks are on the rise. This, coupled with increasing disclosure of unauthorized access to sensitive consumer data, as well as lost consumer data files, is taking a steep toll on consumer confidence in transacting electronically. Companies are going to lose the ability to leverage low-cost electronic communications channels with their customers, unless steps are taken quickly to beef up security. Online U.S. commerce growth will be lowered by 1 percent to 3 percent in the next three years, as service providers struggle to find the right solutions that don't inconvenience consumers and are cost-effective to implement.

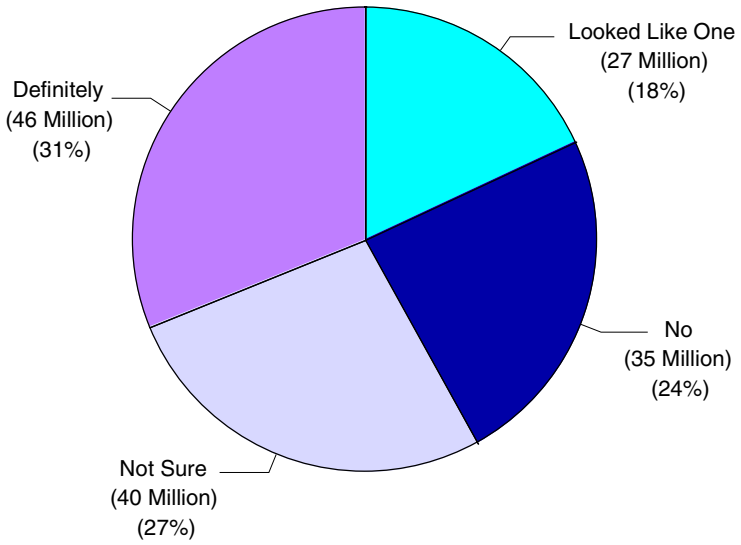
STRATEGIC PLANNING ASSUMPTION(S)

Through 2008, declining consumer confidence will inhibit U.S. ecommerce growth rates by 1-3 percent. (0.7 probability).

ANALYSIS

Phishing attacks grew at double-digit rates last year. In the 12 months ending May 2005, an estimated 73 million U.S. adults who use the Internet said they definitely received or think they received an average of more than 50 phishing e-mails in the past year. That number represents a growth rate of 28 percent compared with the previous 12-month period, during which 57 million U.S. adults reported they definitely received or think they received a phishing attack e-mail. These numbers are according to two consecutive annual surveys Gartner conducted of 5,000 online U.S. adults, who are demographically representative of the online U.S. population (see Figure 1).

Figure 1. Number of Online Adults Who Experienced a Phishing Attack



129146-1

Source: Gartner

Phishing attacks are not subsiding, despite some industry theories that phishing is a fad that peaked in 2004. To the contrary, more than 40 percent of the adults who received phishing attack e-mails received them in the two weeks preceding the survey; another 23 percent received such attacks two weeks before that, which means more than 63 percent of consumers who received one of these e-mails did so in the month immediately prior to the survey. Of the respondents, 95 percent received their last phishing e-mail within the past six months. Present phishing attack prevention methods are obviously not effective; otherwise, these phishing attack e-mails would not be getting through to consumers. Indeed, Gartner is aware of only one Internet service provider (ISP), AOL, which actually blocks identified phishing attacks from its subscribers' mailboxes, rather than merely warning the consumer.

These new numbers are in accord with what major U.S. ISPs and consumer service providers are telling Gartner: Between 150 and 200 uniquely identifiable phishing attacks are targeted against their brands on a weekly basis, which is some four times the level they experienced just six months ago. Those numbers are in fact just what large service providers have identified. No one can be sure how many attacks are not identified; Gartner speculates that more than 30 percent of phishing attacks fall in this category (especially when only one vendor is being used to detect the attacks). This percentage will likely grow as cybercriminals pursue a trend of launching targeted attacks "under the radar" to remain undetected. For example, some phishing attacks evade common security controls by leaving the uniform resource locator (URL) out of the e-mail text and, instead, including it in an e-mail attachment. When the user opens the attachment, a key logger is planted on the user's desktop and records the user ID and password when the user clicks on the URL and enters into a bank Web site (either a legitimate or a spoof site), for example. Key logger scripts then send the user's ID and password to a criminal (unauthorized) server.

An estimated 2.42 million U.S. adults report losing money because of phishing attacks; of those, 1.2 million lost money during the year before the survey. According to these victims, total financial losses this past year amounted to nearly $929 million. (Gartner did not measure this particular number in 2004, but we did report that the 1.8 million adults who recalled providing their financial and other sensitive information to the phishers' spoof sites lost a total of $1.2 billion to identity-theft-related fraud in the year preceding the survey; however, we did not know what amount was a direct result of a phishing attack. In contrast, the 2005 survey specifically asked the victims how much money they thought they lost directly because of phishing attacks.)

Coincidentally, the number of consumers who clicked on the links in phishing e-mails and provided the requested information is almost identical for 2004 and 2005. For both years, nearly 11 million phishing e-mail recipients clicked on the links (or about 15 percent this year and 19 percent last year), and about 1.8 million recall filling in the information requested (or about 2.5 percent this year vs. 3 percent last year). Consumer education efforts are having a marginal positive impact, but that impact is quickly negated by the growing number of online users (148 million in 2005 vs. 140 million in 2004) and attacks. Consumers also endanger themselves just by clicking on a link embedded in a phishing attack e-mail without providing any sensitive data, because the criminal Web site can easily insert malicious software on a user's desktop.

Financial losses and the number of victims this year are likely to be higher than what are reported here; our survey numbers are based on what consumers think they know about the attacks. Many individuals are not even aware that phishing attacks are being launched against them, which results in the theft of their account information and eventually their money. In any event, banks and credit card companies were the main losers in this game — victims said that about 87 percent of their funds were recovered, and financial services companies absorbed the losses in the end.

As was the case last year, PayPal and eBay are still the No. 1 and No. 2 sites that phishers try to spoof, and Citibank is still the primary bank target. But the phishers are turning to smaller regional banks as the larger ones get better at thwarting online criminal activity. The phishers are increasingly pretending to be lottery, sweepstake and similar sites that offer prizes by luring consumers into the chance at winning grand "Las Vegas"-style jackpots.

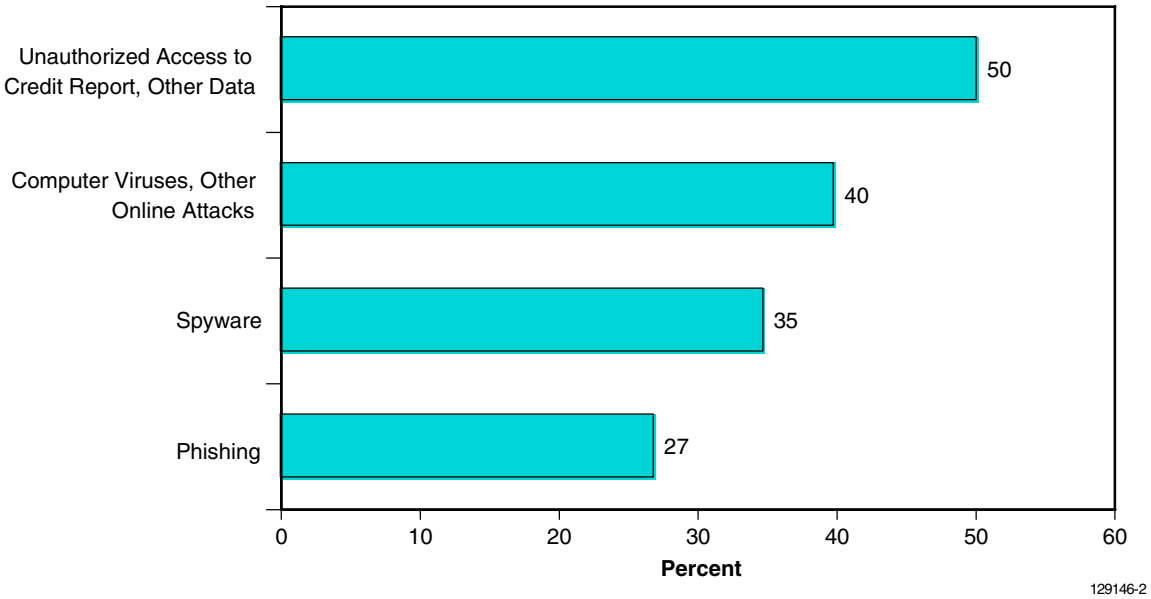
Malicious Software

Despite the increase in phishing attacks, malicious software surreptitiously planted on desktops is an even greater security concern, according to the surveyed consumers. These malicious programs, also known as malicious spyware, or malware, often record the keystrokes of what consumers are typing, such as user IDs, passwords, and credit card and bank account numbers. They also search PCs for other sensitive and confidential information, which the program then transmits to a criminal server. Some 45.6 percent of online consumers report having had malicious software on their desktops, but more than 83 percent also said they had anti-spyware programs running on their desktops. The problem is, however, that anti-spyware programs are not always effective in eradicating malware, especially when there is no signature for the program. For more information, see "A Field Guide to Spyware."

Threats Take a Toll on Consumer Confidence

Consumers are taking notice of increasing cyberattacks, numerous disclosures of unauthorized access to consumer data and misplaced consumer data files, such as well-publicized incidents that occurred in the past six months at Card Systems Solutions, ChoicePoint, Lexis-Nexus, Bank of America, Wachovia and Citibank. In fact, these incidents pose the highest relative concern to consumers, whereas phishing is the least bothersome compared with other attacks (see Figure 2). Nearly twice as many consumers are concerned about unauthorized access to their credit reports and other sensitive data than they are about phishing attacks, even though the latter can certainly lead to the former.

Figure 2. Online Adults "Extremely Concerned" About Fraud and Identity Theft



Source: Gartner

The combined effect of all these attacks is exacting a steep toll on consumer confidence in online commerce. Of the 148 million adults online, more than 77 percent shop online, more than 73 percent bank online, and more than 63 percent pay bills online. With these unprecedented levels of online consumer transactions, companies cannot continue to count on low-cost customer service and marketing channels enabled by the Internet to prevent security breaches.

More than 42 percent of surveyed consumers say their concerns about online attacks such as phishing affect their online shopping behavior. Nearly three-quarters of this group are more cautious about where they purchase goods online, which subsequently adversely affects phishing targets or smaller, lesser-known brands. Nearly one-third of the group buys fewer items than they otherwise would. Consumer concerns have not had as great an impact on online banking, but the effects are still significant. More than 28 percent say that online attacks have influenced their online banking activity; more than three-quarters of this group note that they log in less frequently, nearly 14 percent of them report that they have stopped paying bills via online banking, and more than 4 percent state that they have discontinued online banking altogether.

Perhaps the biggest impact is a newfound and serious consumer distrust of e-mail. More than 80 percent of online consumers — more than 119 million adults — say that their concerns about online attacks have affected their trust in e-mail from companies or individuals they don't know personally. Of these, more than 85 percent delete suspect mail without opening it. This figure has serious implications for banks and other companies that want to use the e-mail channel to communicate more cost-effectively with their customer base. For example, sending a bill electronically costs about half of what it costs to send that same bill through the regular mail. For further details, see "The Big Payoff of Web Billing and Online Customer Service."

All told, Gartner expects the continued growth of online commerce and financial services to be 1 percent to 3 percent lower than it otherwise would be through year-end 2008, until the security of online and electronic information is more heavily safeguarded (0.7 probability).

What Consumers Want When It Comes to Security

Future Gartner research will analyze the survey findings of what consumers want in terms of added security. In general, consumers expect that companies they do business with will provide secure communications and that businesses will routinely protect their data at no extra cost to their customers. Most want their Internet Service Providers (ISPs) to protect them from cyberthreats, although victims who report losing money to phishing attacks favor their banks as the provider here. Nearly 90 percent of surveyed consumers want Web sites to authenticate themselves to the consumer — a feature that is missing from many stronger authentication methods on the market that only authenticate the consumer to the Web site.

Most online consumers don't find the government responsive in terms of protecting them. Only 14 percent believe that the free annual credit reports they are entitled to receive, as recently mandated by the U.S. Congress, is "extremely effective" at protecting them from identity-theft-related fraud. In contrast, nearly one-third are "extremely concerned" that they will suffer some type of identity theft fraud because of incidents such as occurred with ChoicePoint, in which illegitimate businesses gained access to sensitive financial consumer records. Two-thirds of consumers want the government to enact laws that enable consumers to "opt out" of releasing their data to a third party so that the consumer can deliberately specify that such data not be released without their express consent. But opt-out laws go against the interest of the financial services lobby and are therefore highly unlikely to be enacted, despite significant counterlobbying by consumer privacy advocates.

Key Issues

How extensive is identity theft, and what are the applications for fighting it?

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner