Retail Services Industry Relies on Usernames and Passwords Despite Security Threats

Canadian Merchants Slow To Adopt More Sophisticated Online Security Measures, Ipsos-Reid Study Shows

Toronto, June 30, 2005 -- Despite the ongoing commoditization of the Internet, accelerated influx of Web-based services and the availability of sophisticated security software, basic security options such as usernames and passwords are still the leading forms of online security used by merchants, reveals a study from Ipsos-Reid on the payment processing industry.

The independent study shows that 87% of merchants surveyed said they used usernames and passwords as their primary online security option. Firewalls and virtual private networks (VPNs) were the next leading security options preferred by 64% of respondents. Static or dynamic passwords and personal identification (PIN) numbers are used by a reported 51% of merchants.

Although usernames and passwords are not the most failsafe method of security available when used as a primary or singular means of security, this study showed that other more complex security options were not nearly as widely used.

“The increasing adoption of Web-based payment processing may herald the need for both tighter security measures and increased merchant commitment if we are to witness an accelerated adoption of online transaction processing,” said the study’s author, Lise Dellazizzo, vice president of Information Communications Technology for the company.

Security is a Serious Business

The results in the Ipsos-Reid study appear to reflect a relatively slow adoption of more sophisticated and complex security measures developed to fortify security around an increasingly larger and more diverse online transaction environment. At stake is the eventual success of an emerging Web-based payment processing industry and the need for an increased level of trust with users at large, Dellazizzo said.

Although by no means prolific at this point, electronic transaction processing and other supporting Web-based services will likely become increasingly accessible via public and private networks. If merchants are ever to adopt these services en masse, the use of stronger security measures may have to become almost second nature. This notion applies to any electronic environment where transactions and confidential information are being exchanged.

An Ipsos-Reid retail services study, released late last year, showed that the payment processing service area which demonstrated the greatest growth over the next 12 months was online and Internet transaction processing, with a total of 49% of merchants using online processing and 6% more that were projecting to adopt Internet-based transaction processing.

In light of a projected increase in Web-based transaction activity over the coming year, it may be timely for service providers to consider issues around ease of use and merchant acceptance when it comes to wide scale adoption of more sophisticated security measures. The seamless inclusion of deeper and more resilient security features in online processing solutions may be an effective method to stimulate further usage and adoption of these services.

“One of the major barriers to the accelerated adoption of more complex security measures may be a persistent and general lack of knowledge and awareness among merchants of the far-ranging and detrimental effects serious breaches can have on their business”, Dellazizzo said. “Merchant education could be a critical link to increased adoption of more stringent security measures needed to protect both merchants and their customers.”

Leading Threats in the Retail Services Industry

The three leading security risks to online transaction processing are credit card theft, backend hacking and intrusion attacks, based on findings in this wide scale merchant study.

Three quarters (72%) of merchants believe that the risk of stolen credit card information is the greatest threat to online transaction processing overall. Backend hacking used to illicitly obtain payment gateway, password and user information was the next leading threat for 63% of merchants. The risk of network, account and intrusion attacks followed in severity with 60%. The need for data security policies and enforcement was also seen as an important issue for 51% of merchants overall.

The issue of misappropriated credit card information was considerably more pronounced for merchants in the large enterprise segment (with revenues of $100m and above), where 80% of businesses indicated that they considered stolen credit card information a high-risk threat, compared to 72% of total respondents.

“Merchants clearly need implicit reassurance that they can rely on advanced encryption and electronic theft prevention technology. This technology is only as effective as the user allows it to be, however, and unfortunately much of the more advanced security based technology is not in wide use”, said Dellazizzo.

Methodology

Ipsos-Reid completed a study with 500 merchants across Canada in Q4 2004. Merchants were segmented based on annual revenue into five market segments, covering a national spectrum of businesses. The merchants selected to participate in this study were from the retail trade and services sectors. Headquarters were chosen to prevent the duplication of interviews within one company that has multi locations or subsidiaries. Only senior level respondents were chosen for an interview to ensure that we were communicating with the key decision maker, user and buyer of payment processing services. In a sample base of this size, the margin of error was +/- 4.4%.

Source: Ipsos-Reid Payment Processing Opportunity Report

The 2004 Canadian Payment Processing report included an in-depth examination of current and emerging services and technology trends, current and projected usage and adoption trends, an analysis of acquirer mindshare, perception and merchant churn across the retail business community and a review of leading security issues and other primary pain points for merchants in this rapidly evolving industry. Ipsos is launching the 2005 Payment Processing study with an expanded section on security, an examination of merchant reaction to PCI compliance and a SWOT analysis and leadership grid based on merchant perception and usage, as well as retaining the extensive trend analysis done in the 2004 study.

For more information on these reports, visit: http://www.ipsos.ca/goto/2005cppo.cfm

Contact info:
Lise Dellazizzo
416-324-2283
lise.dellazizzo@ipsos-na.com

About Ipsos
Ipsos is a leading global survey-based market research company, owned and managed by research professionals. Ipsos helps interpret, simulate, and anticipate the needs and responses of consumers, customers, and citizens around the world.

Member companies assess market potential and interpret market trends. They develop and build brands. They help clients build long-term relationships with their customers. They test advertising and study audience responses to various media. They measure public opinion around the globe.

Ipsos member companies offer expertise in advertising, customer loyalty, marketing, media, and public affairs research, as well as forecasting, modeling, and consulting. Ipsos has a full line of custom, syndicated, omnibus, panel, and online research products and services, guided by industry experts and bolstered by advanced analytics and methodologies. The company was founded in 1975 and has been publicly traded since 1999. In 2004, Ipsos generated global revenues of € 605.6 million ($752.8 million U.S.).

Ipsos-Reid is an Ipsos company, a leading global survey-based market research group. To learn more, visit www.ipsos.ca.