Mobility Madness

Michael Peters | March 14, 2011

Michael Peters, Chief Information Security Officer

Securely Extending Commerce to Mobile Users

With any emerging information technology, particularly those that interweave financial transactions, such as commerce and banking, one of the first concerns should be security. With an exponentially increasing number of consumers using mobile payment technologies, there is increased scrutiny of the precautions retailers are taking to guard these transactions.

For retailers with mobile commerce sites or applications, not much fundamentally has changed. Retail transactions still take place over the Internet and involve a credit card, a debit card or some alternative payment processing tool such as PayPal. Transactions are treated the same as if they came from an e-commerce site.

Beyond doubt, retailers should apply the same protections to m-commerce as to e-commerce. While mobile payment technologies offer a convenient new vector to pay for a retailer's goods and services, consumers may be at risk of losing money when mistakes are made by merchants and their credit card processors or even by fraud perpetrated by companies' own employees.

On that note, the one major difference between e-commerce and m-commerce for retailers that offers smartphone applications is that some are designed to store payment information within the application. So, if the phone is lost or stolen, the information may be at risk. Even if your smartphone is not lost or stolen, the threatscape for smartphone hacks and malicious software already exists and will only increase. At the very least transactional information should be protected with both encryption and a password, or for even better security, stored and accessed through an e-commerce account where all information resides on a merchant's secure servers.

Current federal law provides some protection to consumers whose credit cards or debit cards are lost, stolen or misused. These protections today are spread across different federal agencies and don't apply to all new types of emerging payment processes. Moreover, commerce conducted in other countries may not be protected.

Industry regulations such as the Payment Card Industries (PCI) regulations only require the very largest of retailers to comply with current security standards, leaving a significant commerce segment to regulate itself. Recently revised PCI security standards do not adequately address m-commerce and the use of modern encryption ciphers. Consumers cannot be expected to understand or to figure out on their own, what security protections apply to each competing new payment mechanism or commerce site.

Regardless of the technology or business organizations involved, the same high level of consumer protections should be guaranteed by law. Unfortunately, laws and regulatory mandates still seem to be many steps behind the marketplace. So it is incumbent upon retailers to implement both their m-commerce and e-commerce sites with consumer security first. In tandem, it is especially incumbent upon suppliers of m-commerce and e-commerce applications to provide inherently secure applications, security-focused implementation services, and aggressive, ongoing security support services to commerce-based companies.

Having devoted my career towards information security and consumer protections, I know what to look for and I know who I trust with my credit card purchases.

Want to know more? Just ask me.