

# Data thieves target smart phones to steal personal information

## Mobile Web increases risk of data breaches

Smart phones are the new battleground for identity theft and fraud, security experts are warning, as businesses and consumers increasingly use mobile devices to transmit sensitive personal information over less secure wireless networks.

## Criminals follow the "smart" money

"With the explosion of smart phones, people are sending more private information over the mobile Web for business, shopping, banking and other applications," said Mark MacGougan, HSB vice president for identity theft and data breach programs. "Hackers and criminals are following the money and scheming to steal that personal data."

## Smart phones in widespread use

One in three American adults now owns a smart phone as the number of smart phones shipped to retailers surpassed personal computers for the first time in 2011. Smart phones have become a standard business tool, meanwhile, with some smaller companies even successfully running their entire operations with mobile devices.



## A powerful storage device for personal information

It's the growing capacity of smart phones to store and transmit personal and financial data that is increasing security risks. Mobile payments make it easy to purchase goods and services and share business information on the go, but cell phones loaded with personal and company data are easily lost or stolen and many people don't use password protection.

## Hackers invade wireless networks to steal data

Smart phones, like laptop computers, can also provide a channel for hackers to invade company servers and steal personal and corporate information. Yet data security strategies are not keeping up as many businesses issue mobile devices to their employees without taking even basic measures to safeguard confidential records.

## Workers use smart phones for business and social activities

The problem is growing worse. One study found that nearly half of employees were allowed to connect their personal mobile phones to corporate systems and 70 percent of employees were allowed to use corporate owned computing devices for personal activities.

## Small businesses risk their bottom line and reputation

Another survey showed that nearly half of small business owners report that they own smart phones themselves. A data breach from a mobile phone or other source can threaten their company's profits, customer base and reputation. And many smaller businesses lack the resources and expertise to protect the information they keep.

## Consumers worry about ID theft and fraud

Consumers worry about identity theft and fraud. Virtually every business is at risk of a breach of the personal information they store on customers, employees and others. When personal data is lost or stolen, most states require that a business notify the people affected.