DATAART

CRMBuyer™
The Essential Guide
For CRM System Purchasers

Getting Your Mobile CRM Mojo Working

As companies rush to offer mobile CRM apps to their customers, they are in danger of repeating the same mistake made a generation ago with the launch of early online initiatives: not placing enough emphasis on security. We know how that worked out. Untold millions of customers were compromised financially because the companies they chose to do business with online did not take proper precautions.

The good news is that some companies remember this history and are taking pains to avoid repeating it as they roll out mobile CRM apps.

"Companies are learning that they have to treat mobile app development just as you would any kind of app development," Alan Goode, managing director of Goode Intelligence, told CRM Buyer.

App Insecurity

In the early days of mobile app development, many companies applied a less rigorous methodology for security, he said. Even a few years ago, the mobile phone was not widely recognized as a serious vector for hackers.

"Now we are seeing a bit of maturity on the part of organizations, as they become increasingly aware of the threats that are out there for mobile users," Goode said.

However, a lax attitude is still evident among some providers.

"I think you can expect major publishers to be very good at — and conscious of — security," Alexei Miller, executive vice president ofDataArt, told CRM Buyer.

"What is harder to control are the emerging startup applications that are making a huge push into the market with their simplicity and ease of use."

Rules of the Road

A good starting point for any company building a mobile app is to design it so that no sensitive data is ever stored on the actual device, Miller suggested.

DataArt's speciality is banking applications. They "need to be designed so even though they allow users to perform sensitive money operations on their smartphones, at no time will the Social Security or bank account number be stored on the device itself — even if it is encrypted," Miller explained.

Frequent security updates — an annoyance on the desktop — work in the mobile provider's favor, because consumers generally accept all updates offered, Tim 'TK' Keanini, chief research officer for nCircle, told CRM Buyer.

"Every app vendor should make security a priority in the design process and then update the app often," he said. "Frequent updates raise the cost of attack to cybercriminals, because even if they find a vulnerability, the window of opportunity is extremely short."

Wireless carriers are also playing a role in mobile CRM security — a big role, Mobile Posse CEO Jon Jackson told CRM Buyer.

"We see mobile CRM making a significant impact for wireless carriers looking to connect more intimately with their subscribers. And as you know, these carriers are singularly focused on maintaining security and privacy during peer-to-peer communications and transactions," he remarked.

Besides undertaking their own security initiatives, carriers are partnering with vendors such as Mobile Posse for additional services, noted Jackson.

Mobile Posse enables carriers to connect directly with opt-in subscribers on the mobile phone home screen, where messages and promotions are served when the phone is idle, thus avoiding unsecured connections over the mobile Web, email or other types of mobile messaging, he explained.

Tools for an Inquiring Consumer

For the most part, many consumers assume the vendor has taken care of security. However, some have their doubts — or at least want a second pair of eyes on what is being downloaded to their devices, said Alex Horan, product manager at CORE Security.

For that, they turn to the security community.

"We spend our time looking at how these applications work, or in many cases, don't work," Horan told CRM Buyer.

Researchers routinely look at whether mobile apps use proper authentication or just the ID of the phone, which can be easily spoofed. Also, in a nod to the role mobile carriers play in security, researchers look at whether the traffic is unprotected because the developer has assumed it will be going over the cellular network, he pointed out.

Security researchers "may be annoying to vendors," he said, "but they are an immensely valuable — and free — service to consumers."