



Forum: Gossip ĭ¼ˆé-’è•Šĭ¼‰

Topic: Safest Way to Bank Online? Your Cell Phone

Subject: Safest Way to Bank Online? Your Cell Phone

Posted by: SoutheLily

Posted on: 2009/6/27 1:02:06

Safest Way to Bank Online? Your Cell Phone

Published: 15 Jun 2009 02:40:10 PST

<http://news.alibaba.com/article/detail/technology/100118609-1-safest-way-bank-online%253F-your.html>

So you want to bank safely online? Then ditch your computer and make the transaction via your cell phone instead.

Using a mobile handset for this most sensitive online act might sound counterintuitive, given that phones are prone to being lost or stolen, but your cell phone might actually be safer than your computer for paying bills or checking your statement online.

Some phone malware does exist, and examples tend to make headlines due to their novelty. But the main threats to online security, such as keyloggers, Trojan horses, and other data-stealing software, don't exist for phones--yet.

"The risk of being infected on a mobile phone is tiny in comparison [with a PC]," notes the security firm Sophos in its annual threat report.

Remote Control

Security firms have long marketed antimalware products for mobile phones. One such company, Kaspersky, acknowledges the lack of threat from mobile malware (at least in the United States). Recently, as a way to appeal to the market here, it added the ability to remotely wipe out sensitive data on a lost or stolen handset to its mobile security product.

"There's a whole lot of upside and security advantages to mobile devices," says James Van Dyke, president of Javelin Strategy and Research, a financial services research firm.

Financial services for cell phones are plentiful. PayPal lets you send money to another person via your phone. Companies including Obopay, mChek, and KushCash are joining in. Bank of America, Wells Fargo, and others also offer services.

Cell phones dodge malware because they run many different operating systems. Security experts agree that crooks stand to steal much more by investing their time in writing a new Windows virus that is capable of infecting millions of PCs than in constructing a Trojan horse that can target only a certain type of phone.

Android Danger

But that may change. Google is hard at work on its Android phone OS, and iPhones make their way into more and more pockets and purses daily. So while phone OS consolidation holds great promise for better apps and services, it could also make phones more of a target.

Look no further than the Mac for an example of what may come. Apple's OS is still largely ignored by the bad guys, but its growing popularity means that it's no longer a haven of guaranteed security. Last November, Sophos notes in its report, a Mac user who happened across the wrong Web site risked getting infected by the OSX/RSPlug malware, which sought to subvert Mac network settings and to force any browser used on that Mac toward phishing and ad sites.

Not Out of the Woods Just Yet

The fact that little mobile malware exists does not mean that cell phones are completely safe, of course. Banking and payment systems require passwords and/or PINs, so someone can't just pick up your phone and start transferring money out of your account. But there's still plenty of personal information that someone could obtain through your phone.

Phishing--the other big threat to online financial security--may be even more dangerous for phones than for computers. If you read e-mail on a smart phone, you'll see phishing messages. And whereas on the desktop both Internet Explorer and Firefox employ built-in antiphishing protections, mobile browsers do not.

"You don't have all the antiphishing toolbars" for a mobile browser, says Dave Jevans, chairman of the Anti-Phishing Working Group. Also, some rare attacks twist the traditional phishing message to target mobile phones. Dubbed "smishing" or "vishing" for their use of SMS messages or VoIP systems, such scams may send a phone a text message containing a warning about a credit card account. If you call the number included in the message, an automated VoIP system prompts you to enter your credit card number, for example.

If mobile banking and personal payments catch on, phone-specific risks with malware and phishing may go up as well. "The expectation is that we will see more malicious applications on devices," says Samir Kumar, group product planner for mobile communications business with Microsoft. But for now, he says, the greatest danger arises when phones are lost or stolen.

Phone safety measures, such as locking the device, remain paramount today, especially if you engage in mobile banking, says Kumar. Another tip: Secure your phone's Bluetooth connection by limiting it to known devices.

Go to Page Page 1 of 1 1