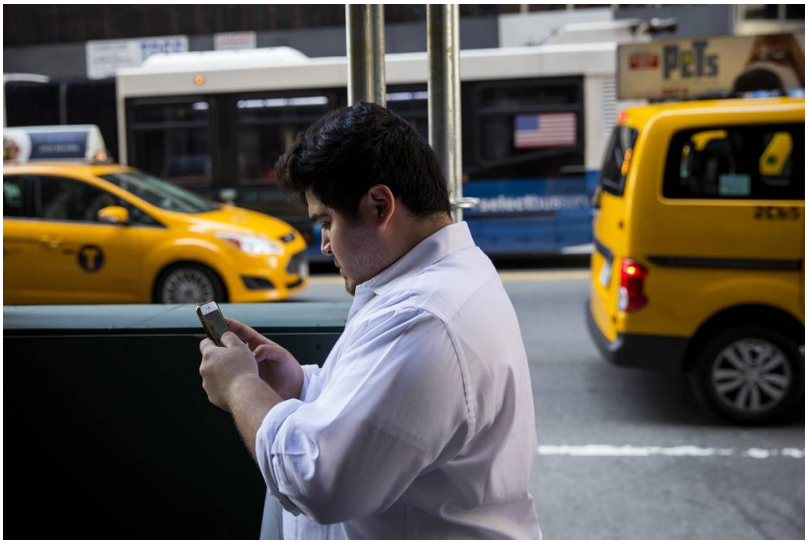
THE WALL STREET JOURNAL.

http://www.wsj.com/articles/mobile-bank-heist-hackers-target-your-phone-1472119200

MARKETS

Mobile Bank Heist: Hackers Target Your Phone

Malicious programs with names like Acecard and GM Bot gain popularity with thieves



A man uses his smartphone in New York in July. *PHOTO: CAITLIN OCHS FOR THE WALL STREET JOURNAL*

By **ROBIN SIDEL**

Aug. 25, 2016 6:00 a.m. ET

Cyberthieves have a new way to hack into consumer bank accounts: mobile phones.

Malicious software programs with names like Acecard and GM Bot are gaining popularity around the world as criminals look for new and lucrative ways to attack the financial-services industry. Cyberthieves are using such so-called malware to steal banking credentials from unsuspecting consumers when they log onto their bank

accounts via their mobile phones, according to law-enforcement officials and cybersecurity specialists.

It is difficult to quantify how much money has been stolen as a result of the mobile-phone malware, mostly because the thieves can access an account through any normal channel after they steal credentials through a phone. Still, the prevalence of the malware is significant enough that it has caught the attention of the Federal Bureau of Investigation and U.S. banking regulators.

The FBI is seeing new types of malware specifically aimed at banking applications for the purpose of stealing account credentials, says Richard Jacobs, an assistant special agent in charge who handles cybercrimes. He has been warning the financial-services industry about the trend, which is typically aimed at large banks.

The Federal Financial Institutions Examination Council, which brings together five banking regulatory bodies, in April updated its guidance for banks to include potential threats facing mobile financial services, including mobile-phone malware.

Ian Holmes, banking fraud solutions manager for security firm SAS, estimates that the Acecard malware has customized overlays to imitate 50 financial-services apps. The malware "is gaining credibility in the criminal underworld," said Mr. Holmes.

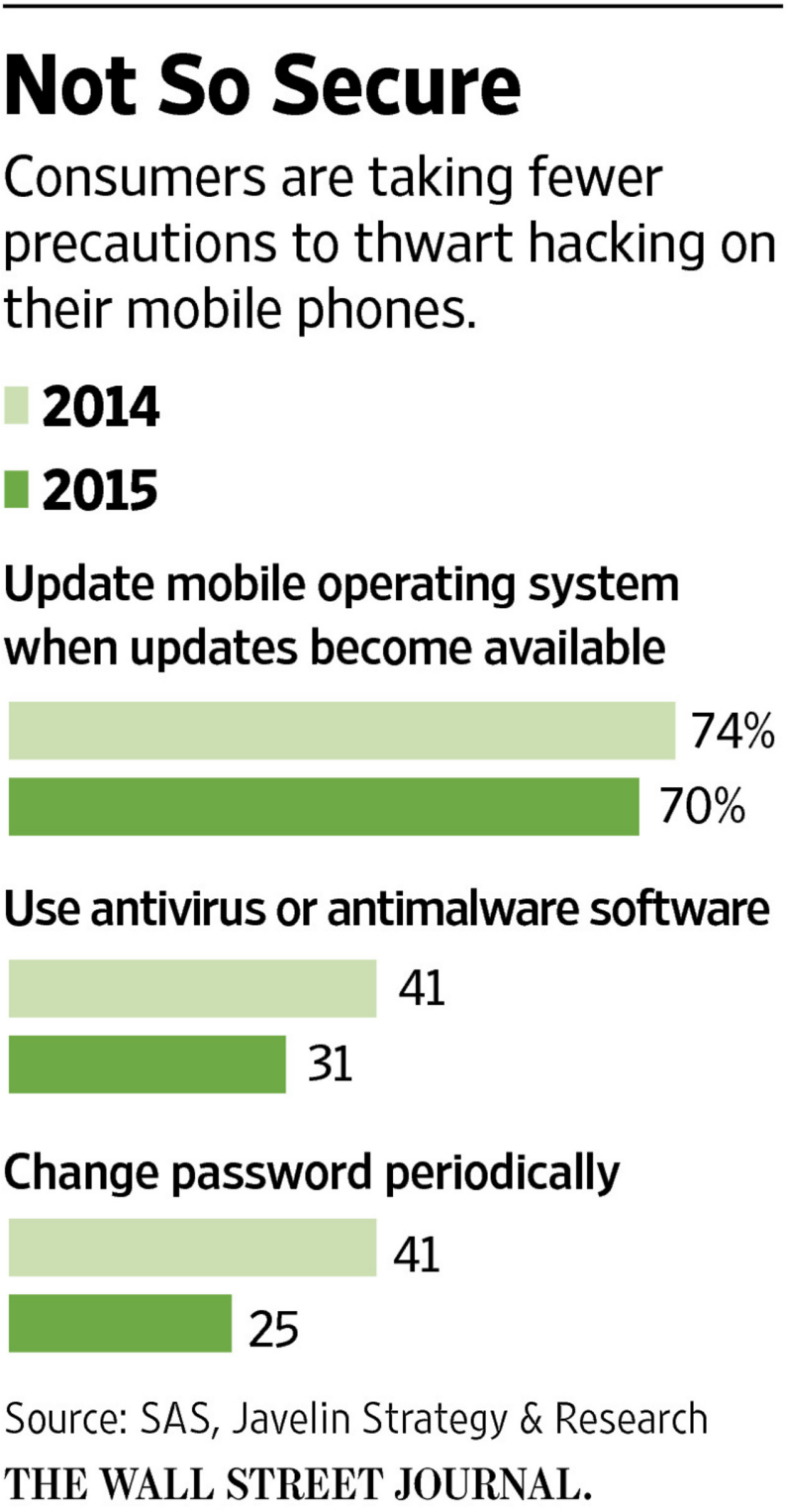
The growing threat represents a new entry point for criminals who typically steal bank credentials by other means, such as installing skimmers on automatic teller machines or by using scams targeting desktop computer users. Meanwhile, a raft of credit-card breaches in the past few years has led to a glut of stolen card numbers. These are being sold on underground websites for as little as $1 each, making them a less profitable business for cyberthieves.

MORE

- 8 Tips to Protect Your Phone and Money From Hacking (http://blogs.wsj.com/moneybeat/2016/08/25/8-tips-to-protect-your-phone-and-money-from-hacking/)

The malware typically gets onto a phone when a user clicks on a text message from an unknown source or taps an advertisement on a website. Once installed, it often lays dormant until the user opens a banking app.

The malware then creates a customized overlay on the authentic banking app. This allows criminals to follow a user's movements on the phone and eventually grab credentials to the account.



This type of mobile-phone malware is gaining ground as more consumers are using banking apps and financial firms are rolling out a wider array of mobile services.

The Federal Reserve said earlier this year that 53% of smartphone users with bank accounts had used mobile banking in the previous 12 months, up from 43 % in 2011. The most common mobile-banking activity is checking an account balance.

Mobile phones are considered particularly vulnerable to hackers because consumers typically don't install anti-malware protection onto their devices.

A recent study conducted by SAS and Javelin Strategy & Research found that fewer than one-third of smartphone owners use mobile antivirus or anti-malware software on their phones. Additionally, some mobile-phone owners unknowingly make their devices

vulnerable to attacks when they tamper with operating systems to run unauthorized apps.

“As a bank, you can have all the protections you want, but unless there is protection on the device, you can’t protect against this kind of attack,” says Ross Hogan, global head of the fraud prevention division at Kaspersky Lab, a cybersecurity firm.

The rising popularity of mobile-banking malware creates yet another security headache for consumers who are increasingly turning to their mobile phones for everyday tasks from banking to shopping.

It also represents a setback for banks that are pushing customers toward digital channels as a way to reduce costs and improve efficiency. Banks typically reimburse customers for money stolen from their accounts, particularly if they notify the institution quickly after the theft occurs.

In some cases, the malware adds fields that request the customer’s date of birth or Social Security number, says the FBI’s Mr. Jacobs. Some of the more advanced forms of malware can even track verification codes that the bank may send to the customer in a text messages as a secondary authentication, cybersecurity officials said.

Once the malware captures a phone user’s banking credentials, it can send them remotely to the criminal, who can use them or sell them.

Some of the bank-specific malware sells for as much as $15,000, according to people who are tracking the trend.

Bank executives say they are trying to thwart the malware by frequently updating and revising their banking applications.

They also say that the banks’ security systems can often trigger alerts for unusual behavior, such as a large withdrawal or if the account is accessed from a previously-unknown device or an unfamiliar location. In such cases, the bank may require additional authentication from the user.

Still, the crimes can be difficult to track because customers mightn’t notice that a theft has occurred until well after they used their phone to log onto the account. In addition, customers may be unlikely to consider their mobile phone as an entry point for hackers if it hasn’t left their possession.

Write to Robin Sidel at robin.sidel@wsj.com

What To Read Next...

HEALTH

Mylan Faces Scrutiny Over EpiPen Price Increases

RELATIVE VALUES

Three Homes for Sale With Lavish Bathroom Vanities

HOUSE CALL

Hamilton Biographer Ron Chernow Finds New York's 'Quietest' Home

EUROPE NEWS

Italy Earthquake Death Toll Rises to 247 People