

# Minimizing the Threat of Mobile Banking Cybercrime

SESSION ID: MBS-T10

Paul J.S. Oliveria

Technical Communications Manager  
Trend Micro Incorporated

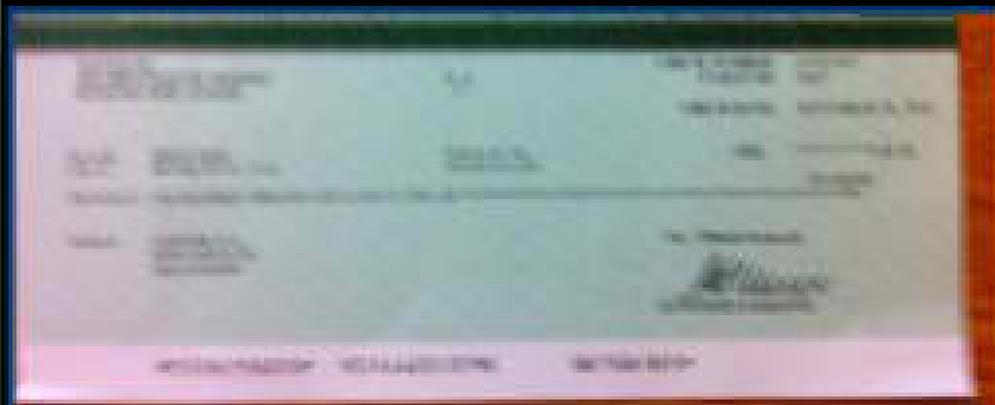


Back

## Photograph Check Front



Make sure the entire check is inside the blue box and touch the camera icon when you are ready. Your iPhone will take the picture when the phone is steady.



# Krebs on Security

In-depth security news and investigation



BLOG ADVERTIS

## 17 Double Cashing With Mobile Banking

JUN 13



The case of a Kentucky man arrested this month for using mobile banking to steal thousands of dollars from a local supermarket chain highlights the security loopholes that thieves can exploit in mobile check deposit schemes being deployed by financial institutions across the country.

Louisville, Ky. based news station **WDRB Inc.** carried a story last week about a local man who was arrested after allegedly using mobile banking to steal more than \$12,000 from multiple Kroger stores.

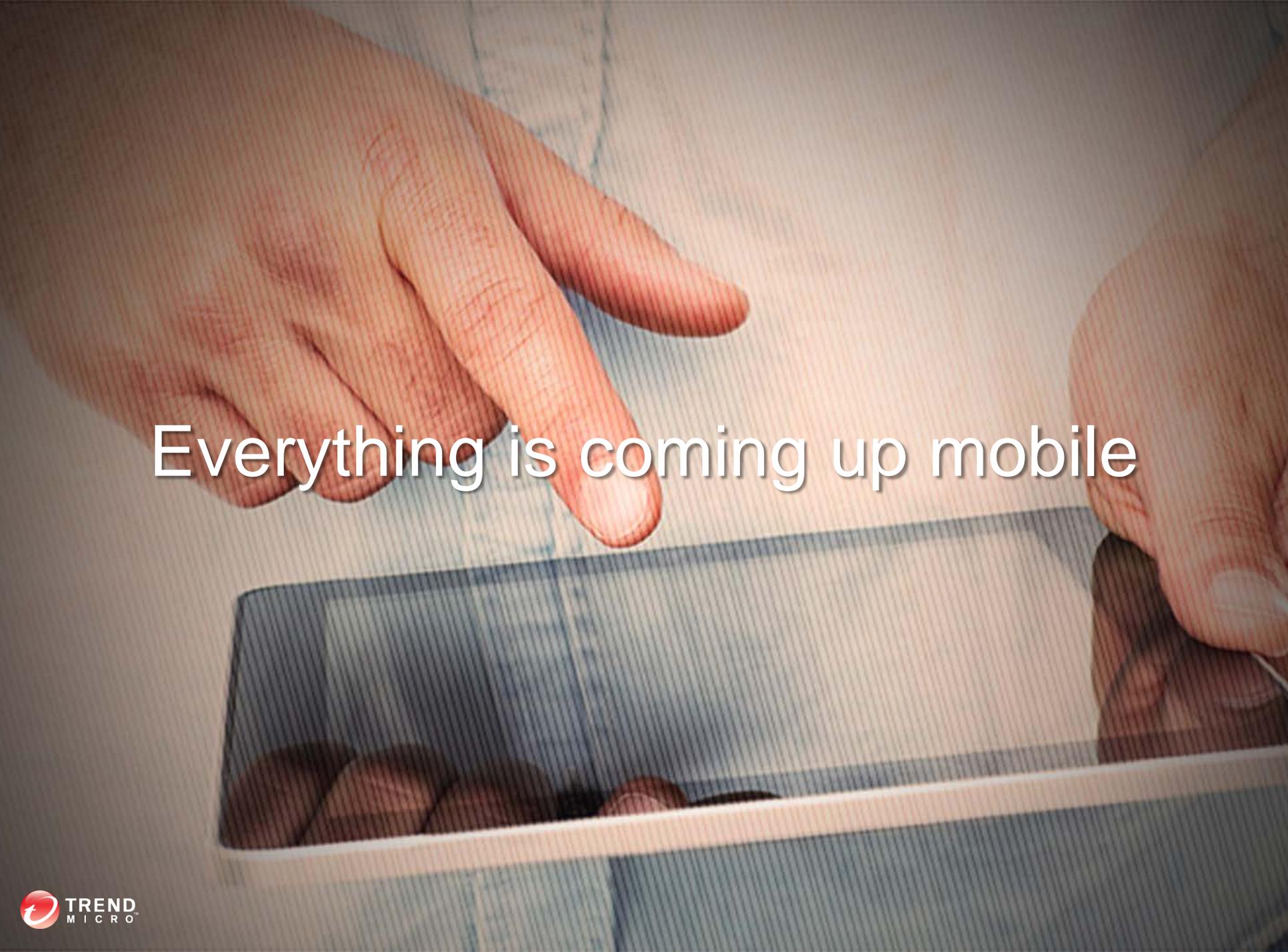


Advertisement



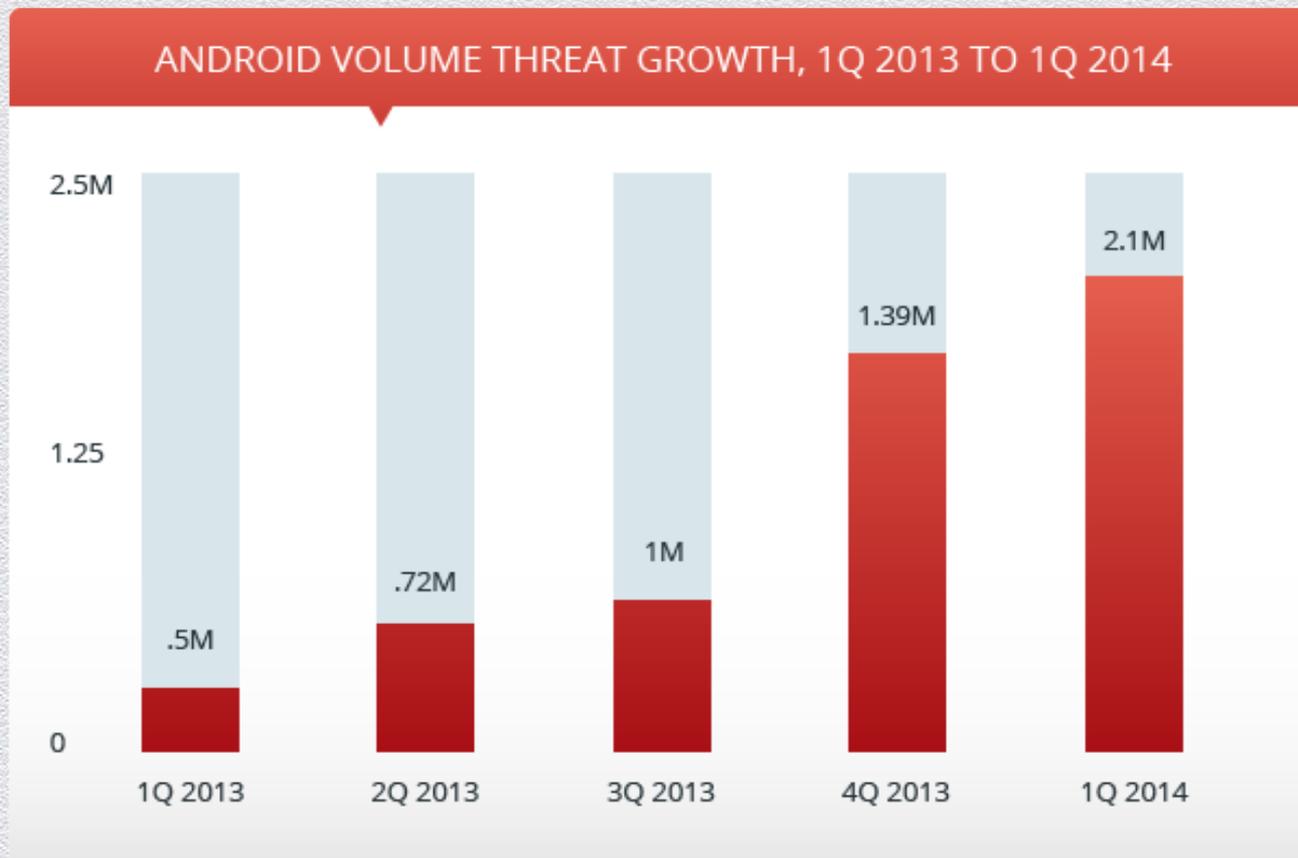
How to D  
and XSS  
SIEM Eve

W A

A close-up photograph showing a hand on the left pointing its index finger towards a smartphone held by another hand on the right. The phone is held horizontally and is the central focus of the image. The background is a light-colored, textured surface.

Everything is coming up mobile

# Android Threat Volume



# Mobile Cybercriminal Underground

A Trend Micro Research Paper

CYBERCRIMINAL UNDERGROUND ECONOMY SERIES

## The Mobile Cybercriminal Underground Market in China

Lion Gu  
Forward-Looking Threat Research Team

Cybercriminal Underground Wares Sold in China		
Internet short message gateway spamming service	5,000 text messages	RMB 300 (~US\$50)
	10,000 text messages	RMB 400 (~US\$65)
	20,000 text messages	RMB 700 (~US\$115)
	50,000 text messages	RMB 1,500 (~US\$250)
	100,000 text messages	RMB 2,800 (~US\$460)

中国移动 9:59 89%

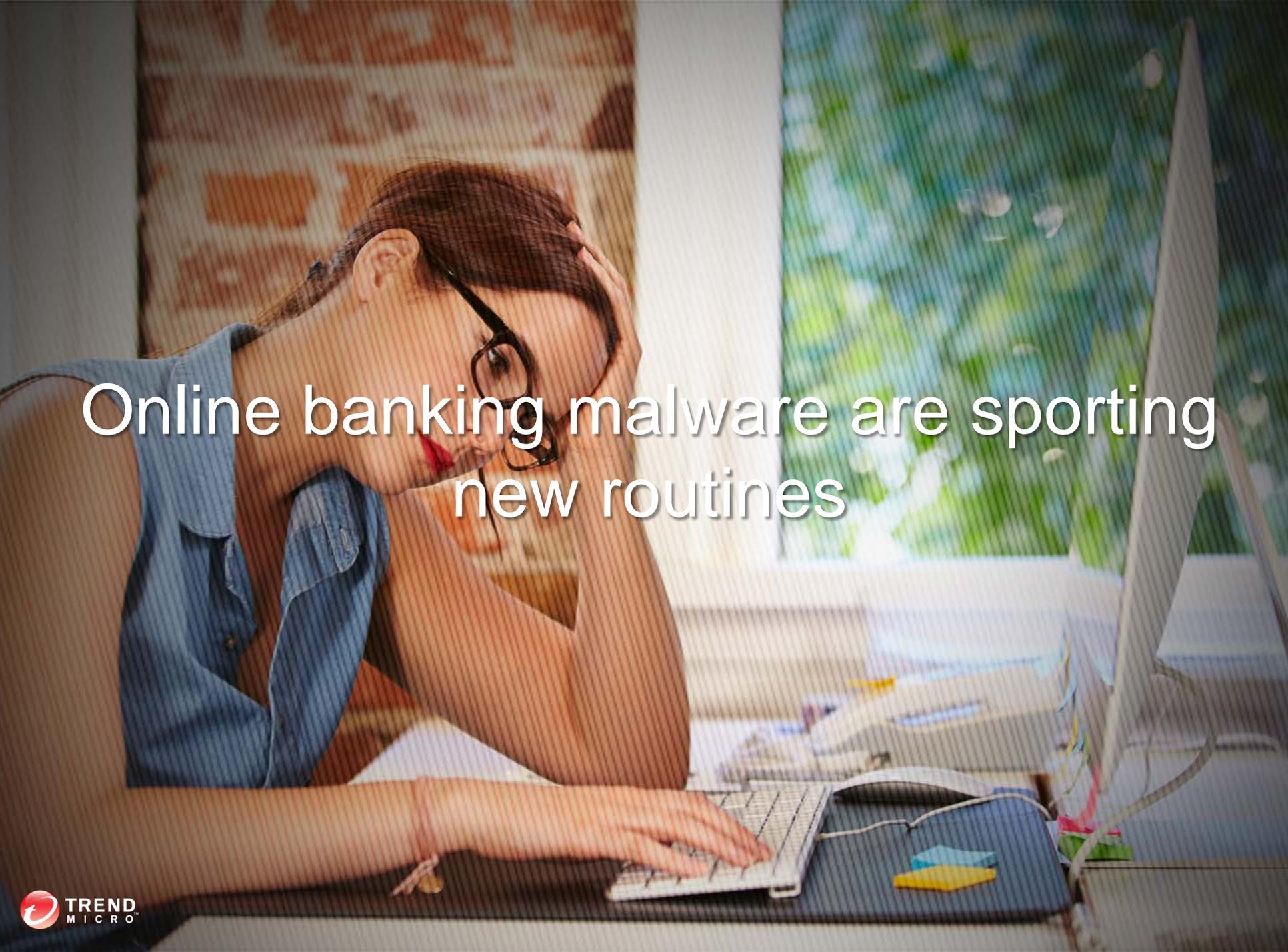
信息 编辑

呼叫 FaceTime 添加联系人

短信/彩信  
2013-7-31 9:32

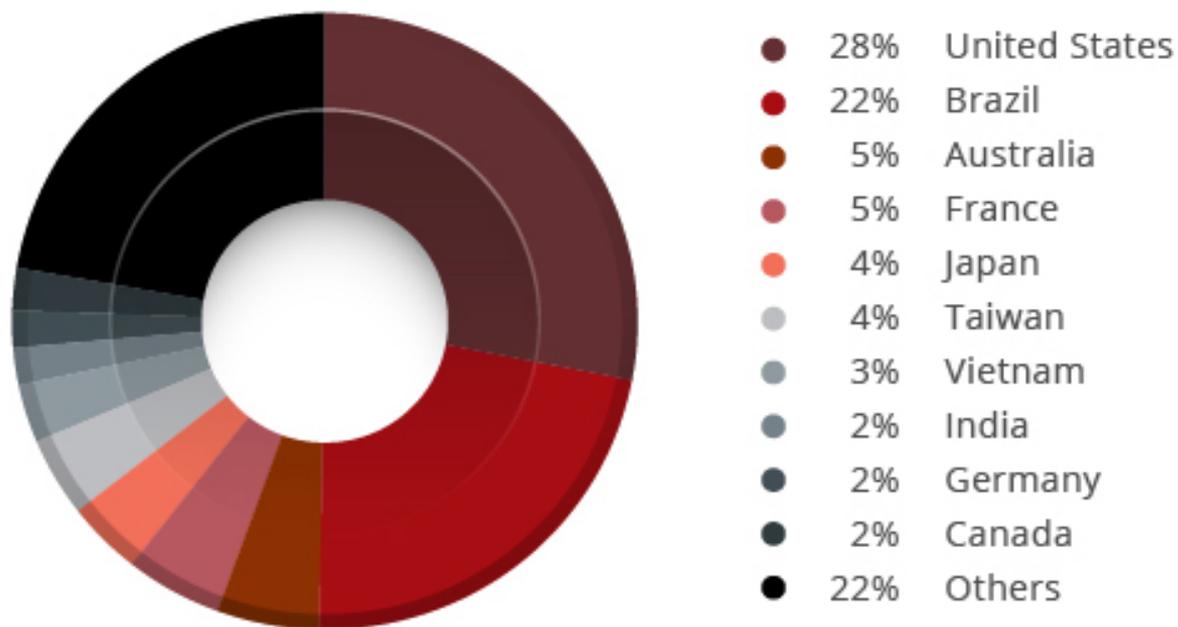
您好：您的电子密码器将于次日过期请尽快登路我行网站 [wap.icbcyt.com](http://wap.icbcyt.com) 进行更新！给您带来不便敬请谅解 工行 (95588)

Your password in ICBC Bank will expire tomorrow. Please change password in website: [wap.icbcyt.com](http://wap.icbcyt.com) as soon as possible. Sorry for any inconvenience. ICBC (95588)



Online banking malware are sporting  
new routines

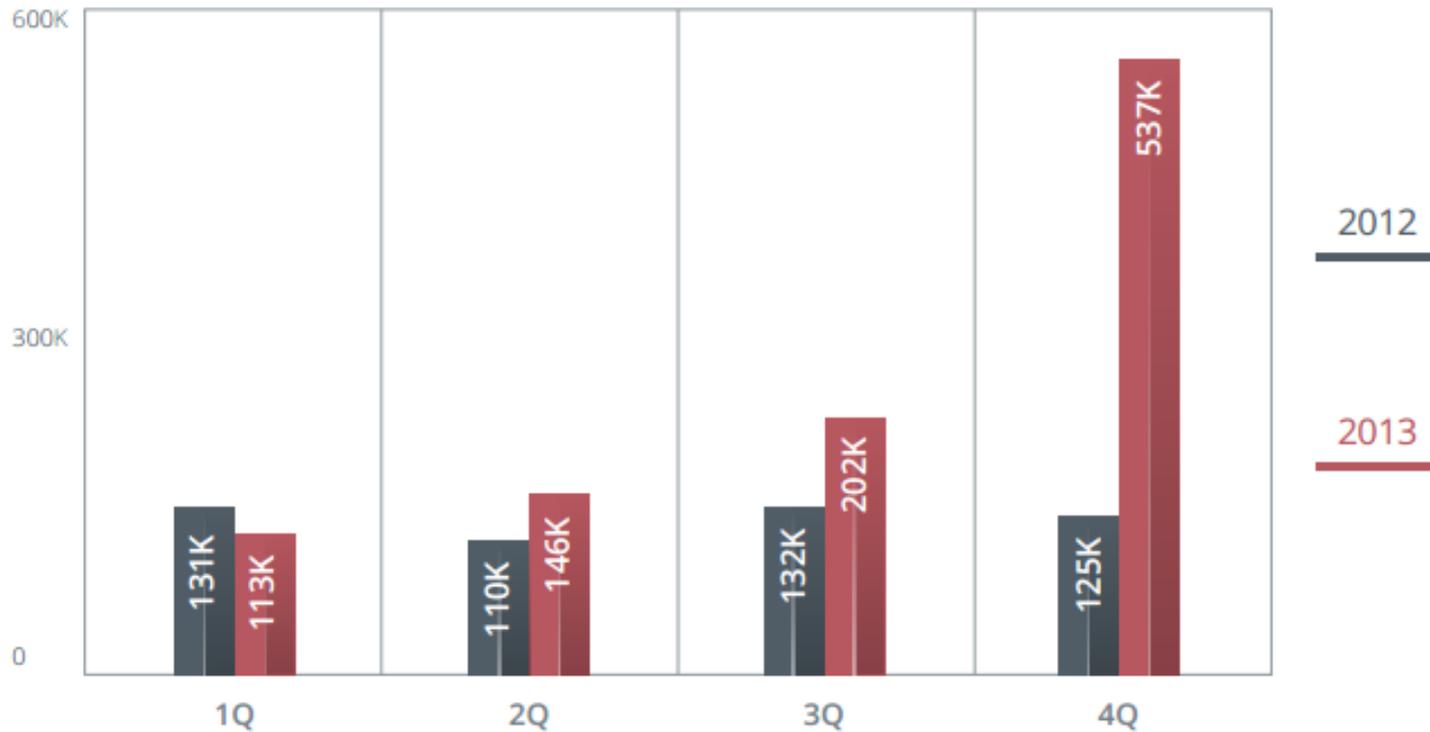
## Online Banking Malware Infections by Country



## Online Banking Infections by Country

*Based on 2013 Trend Micro Smart Protection Network Data*

## Total Online Banking Malware Volume, 2012 and 2013



## Total Online Banking Malware Volume 2012 vs. 2013

*Based on 2013 Trend Micro Smart Protection Network Data*

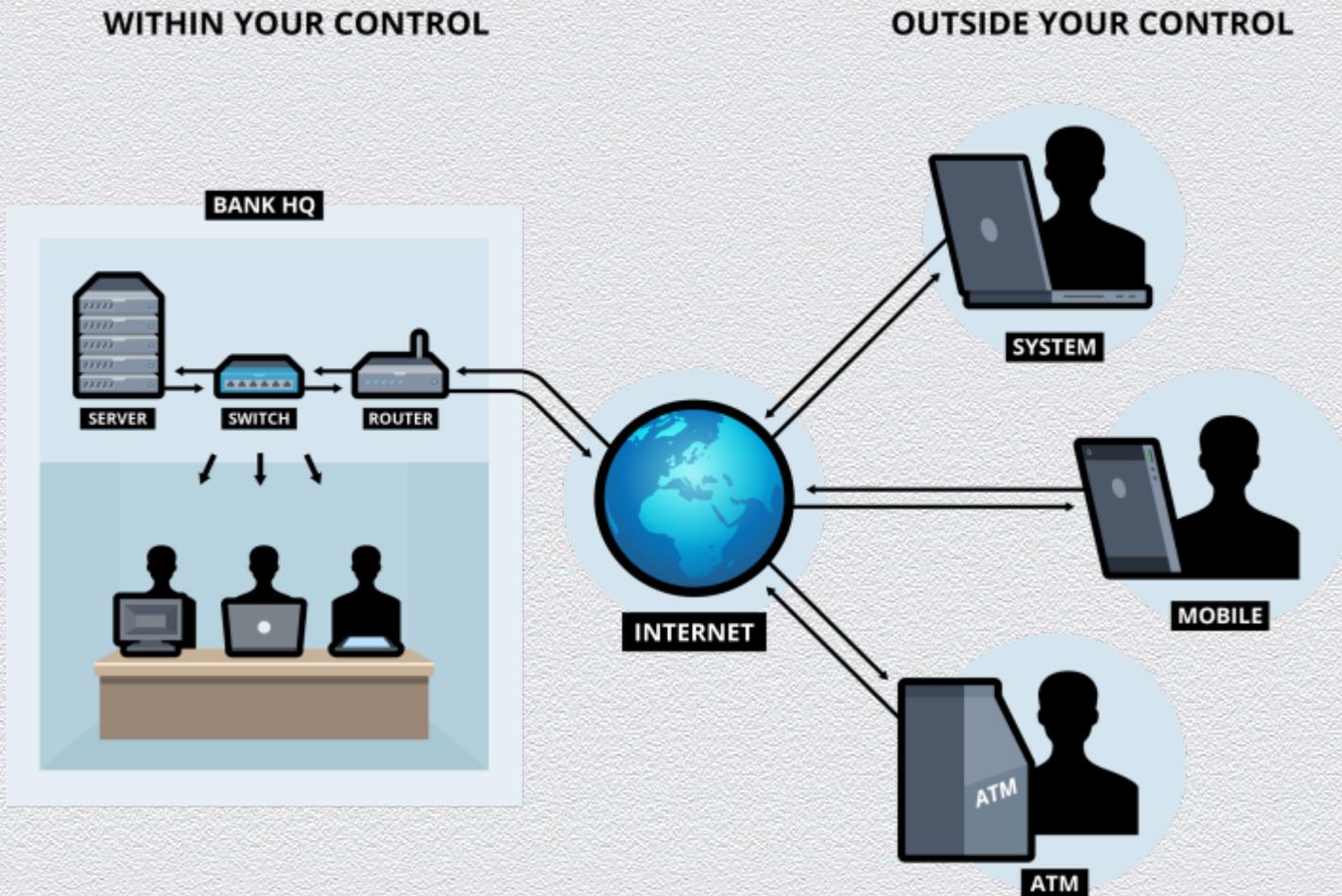


Mobile + Banking = A Perfect Storm

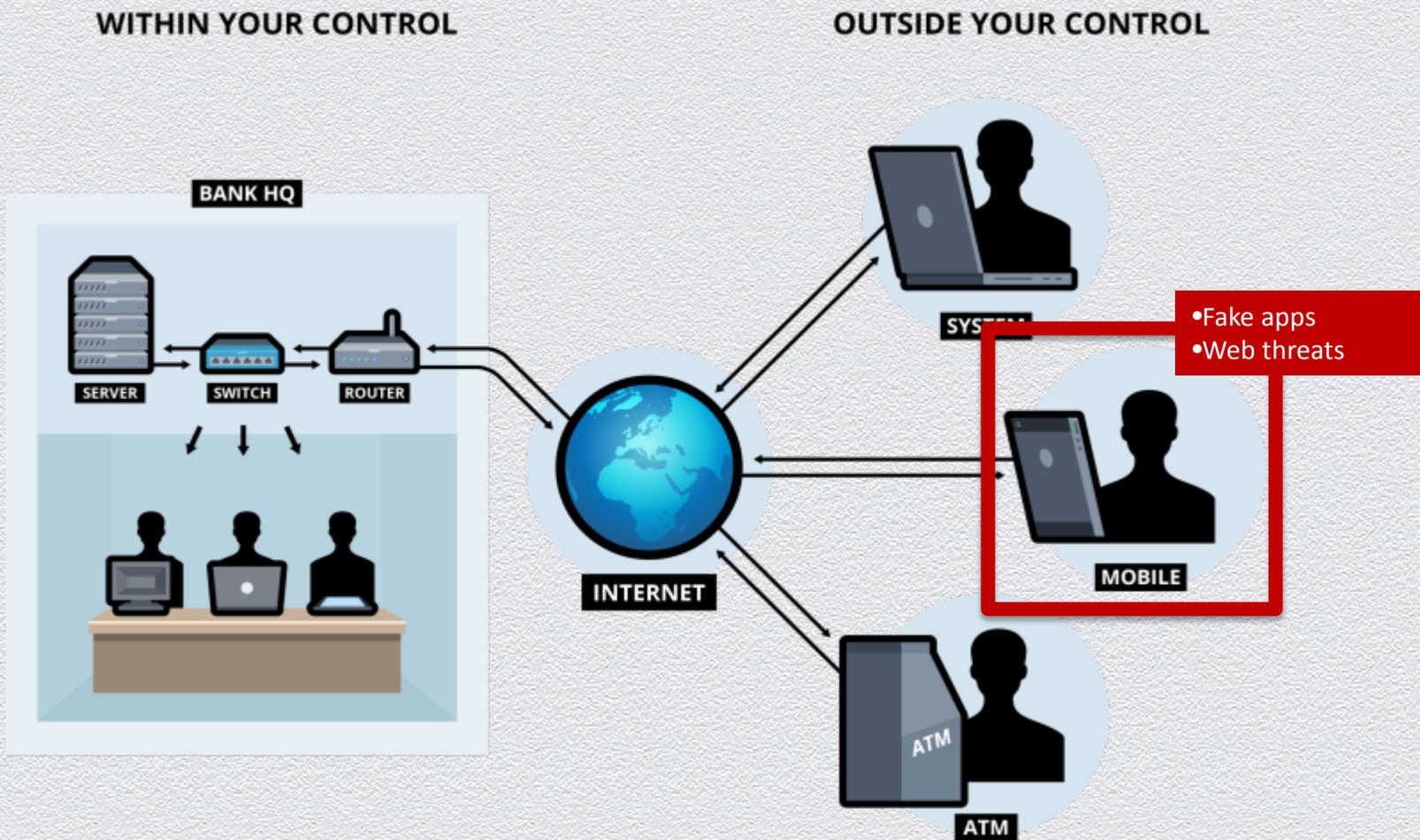


## Security Risks in Mobile Banking

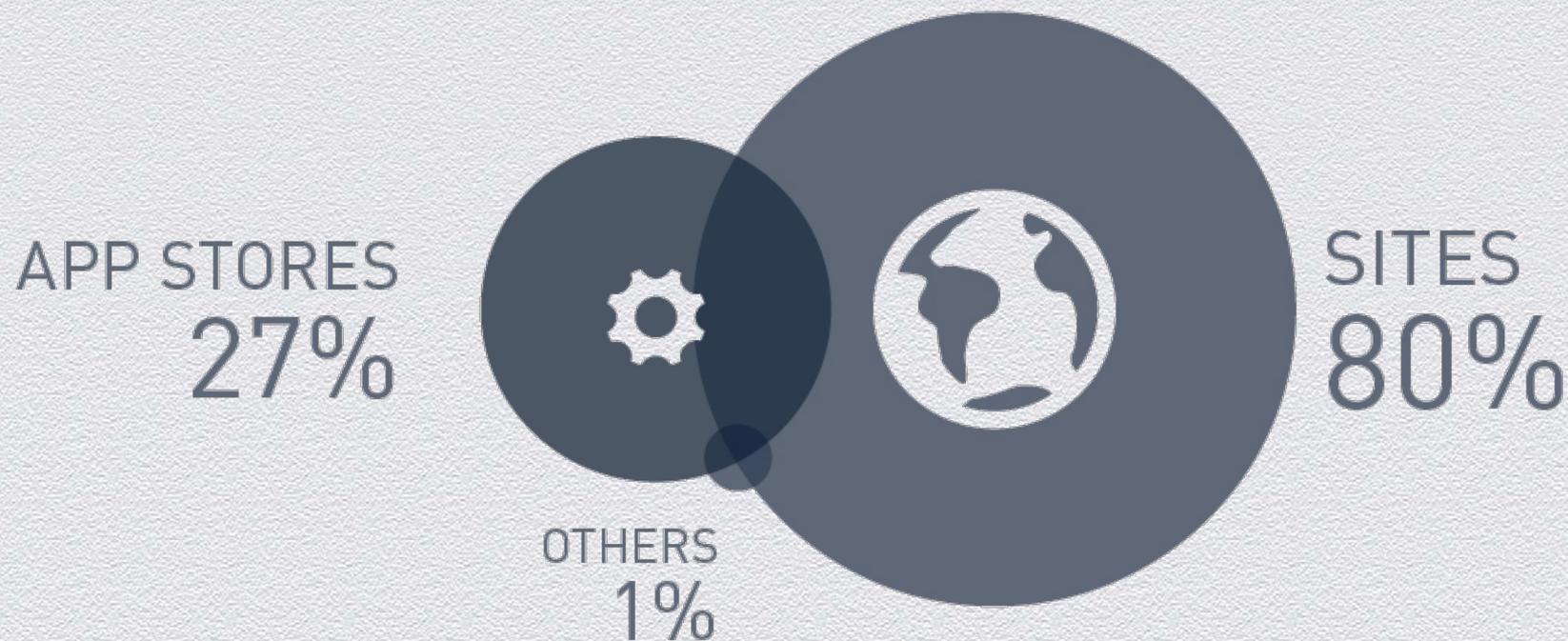
# Entry Points for Security Threats



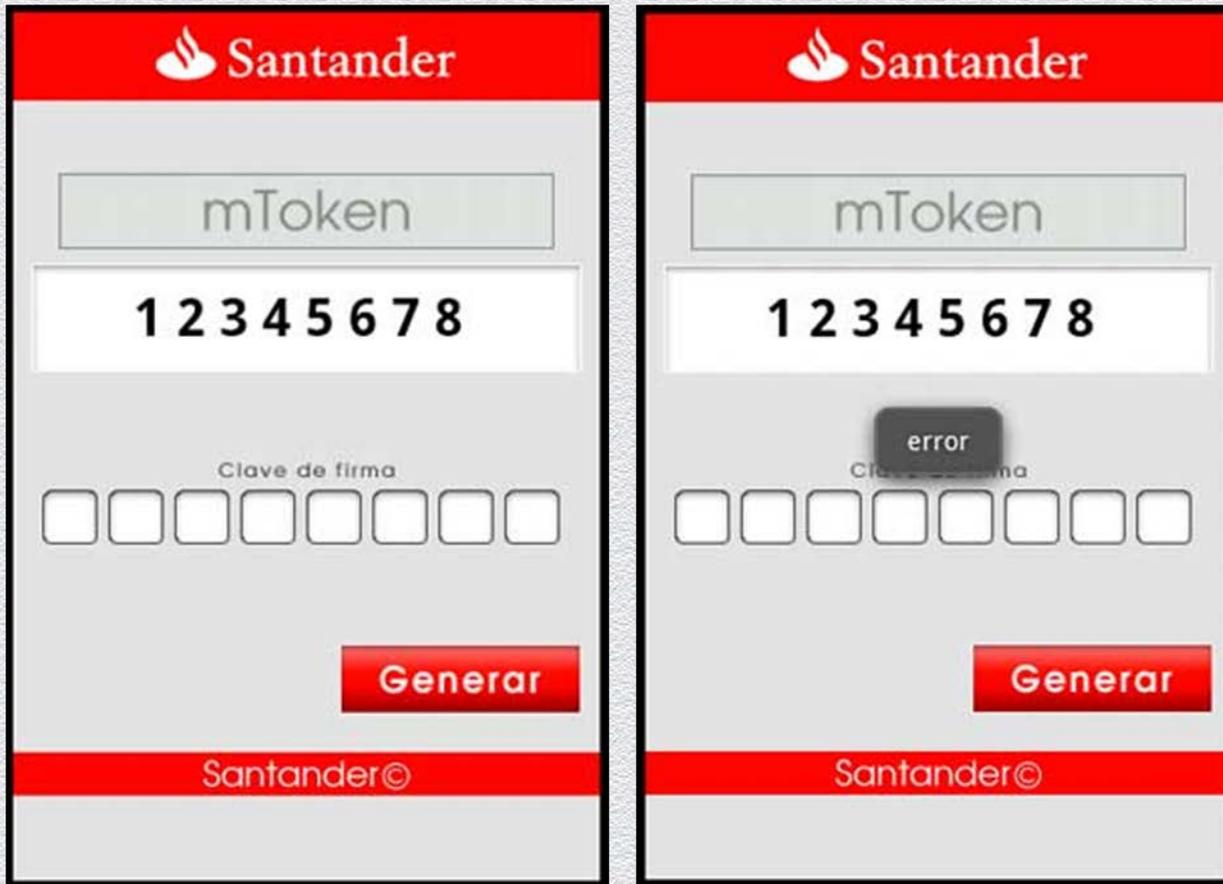
# Entry Points for Security Threats



# Where Users Stumble Upon Malicious Apps

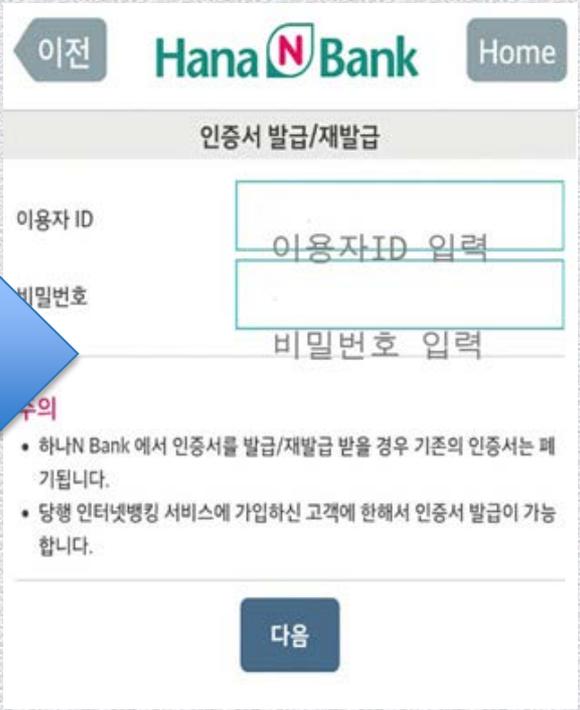
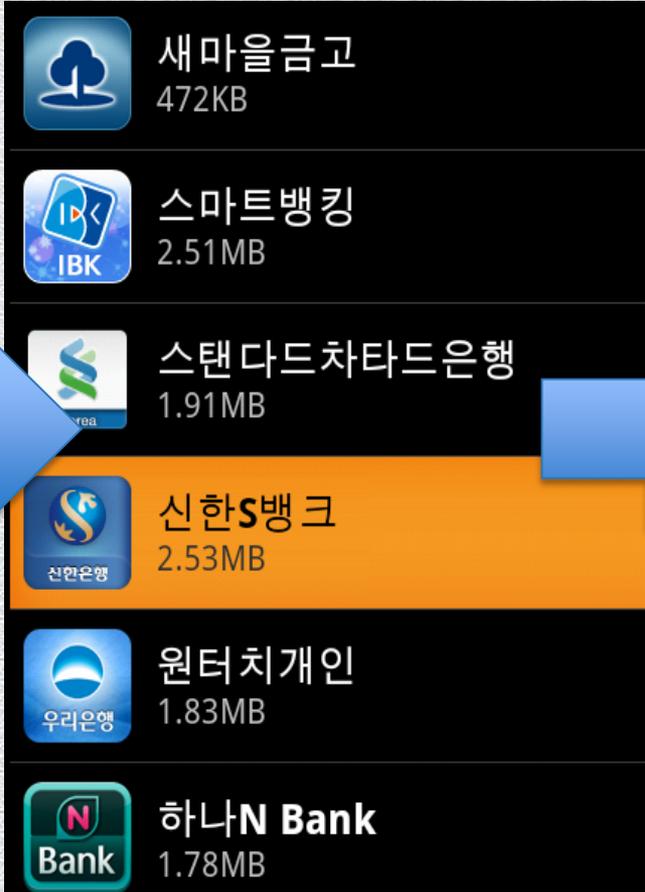
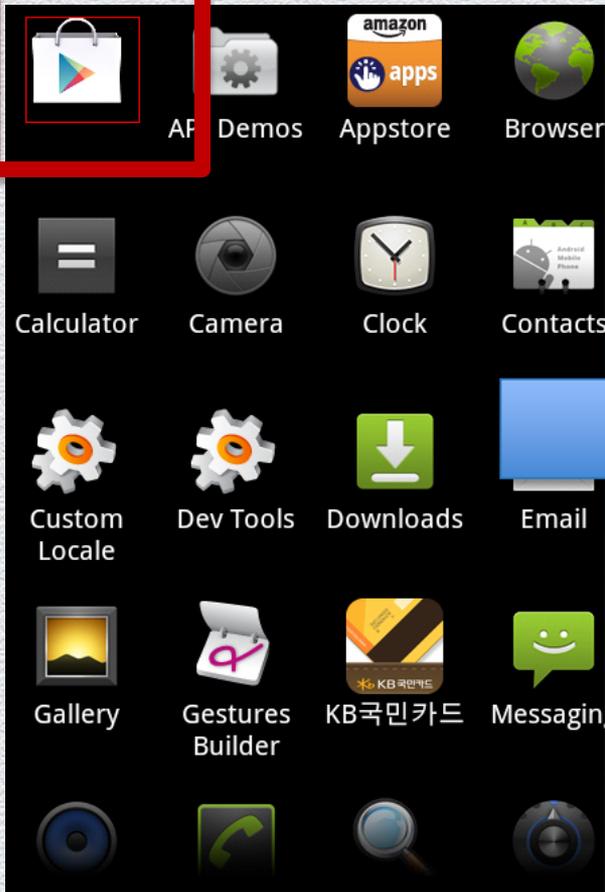
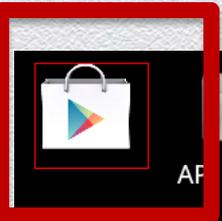


# Fake Banking Apps



- ◆ Fake token generator app steals bank password and sends user and device information (e.g., SMS, contact lists, etc.) to a remote server.

# Fake Banking Apps



# “Trojanized” Banking Apps

InformationWeek  
**DARK**Reading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home News & Commentary Authors Slideshows Video Radio Reports White Papers EV

ATTACKS/BREACHES APP SEC CLOUD ENDPOINT MOBILE PERIMETER RIS

## VULNERABILITIES / THREATS

8/6/2013  
10:58 AM

### Android Trojan Banking App Targets Master Key Vulnerability

**Sluggish Android updates put users at risk. Could rising public awareness of the flaw lead carriers and device makers to patch more quickly?**



Mathew J. Schwartz  
News

Connect Directly



4 COMMENTS

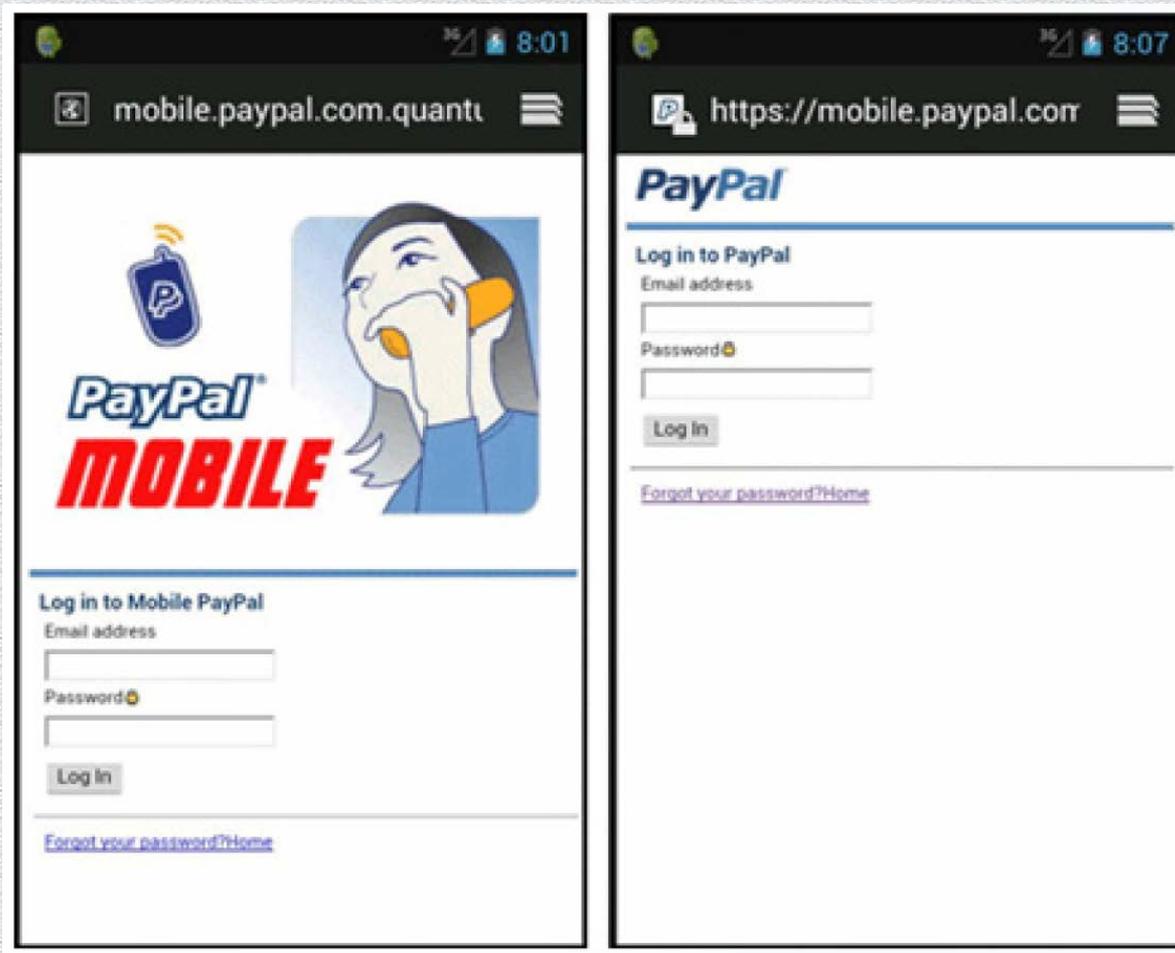
Security researchers have spotted a legitimate banking app for Android smartphones and tablets that has been “trojanized” using the so-called master key vulnerability. That flaw, which affects all versions of Android prior to version 4.2.2, can be used by attackers to inject malicious code into a digitally signed, legitimate Android app.

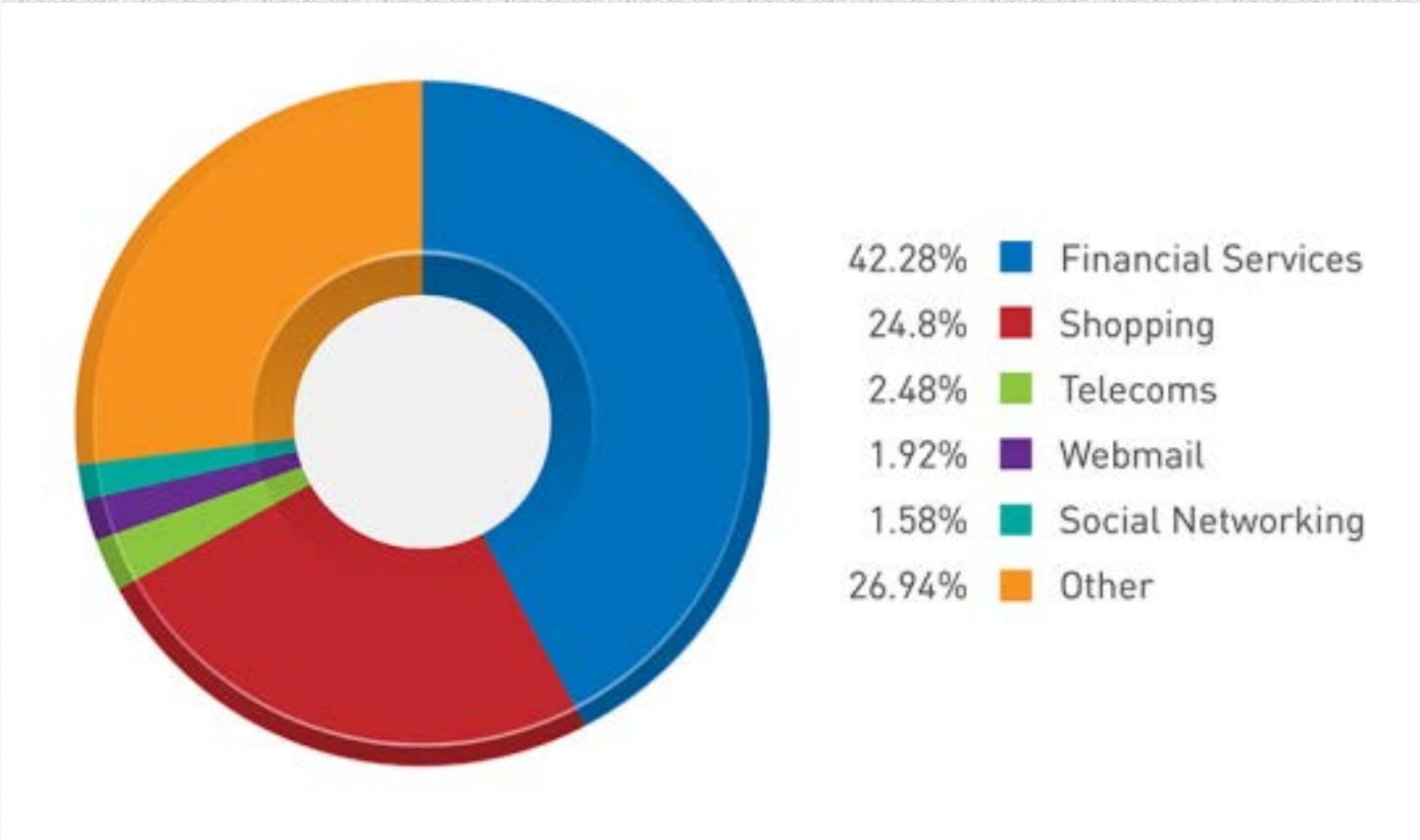




Apps are just one piece of the puzzle.  
Threats continue to transition from PC  
to mobile with help from malicious  
URLs.

# Mobile Phishing

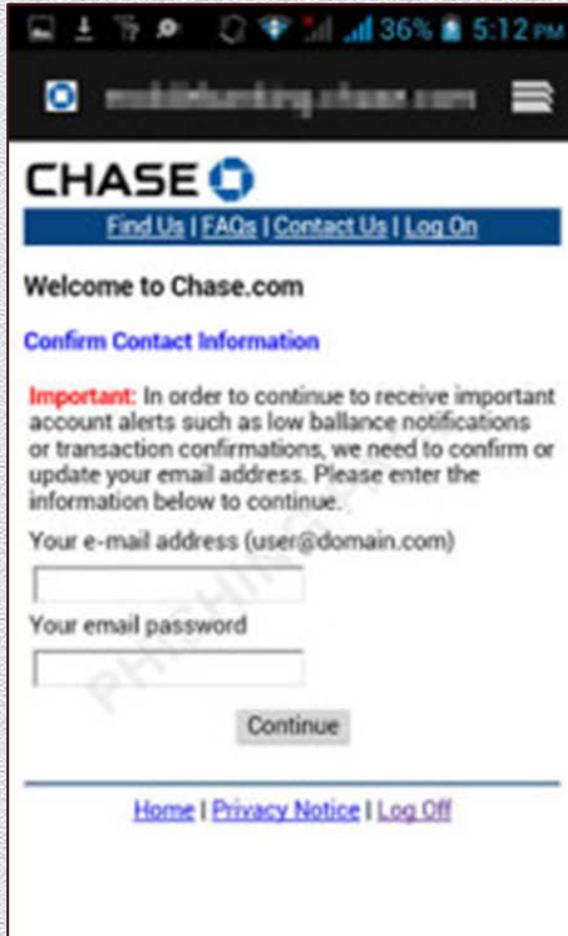




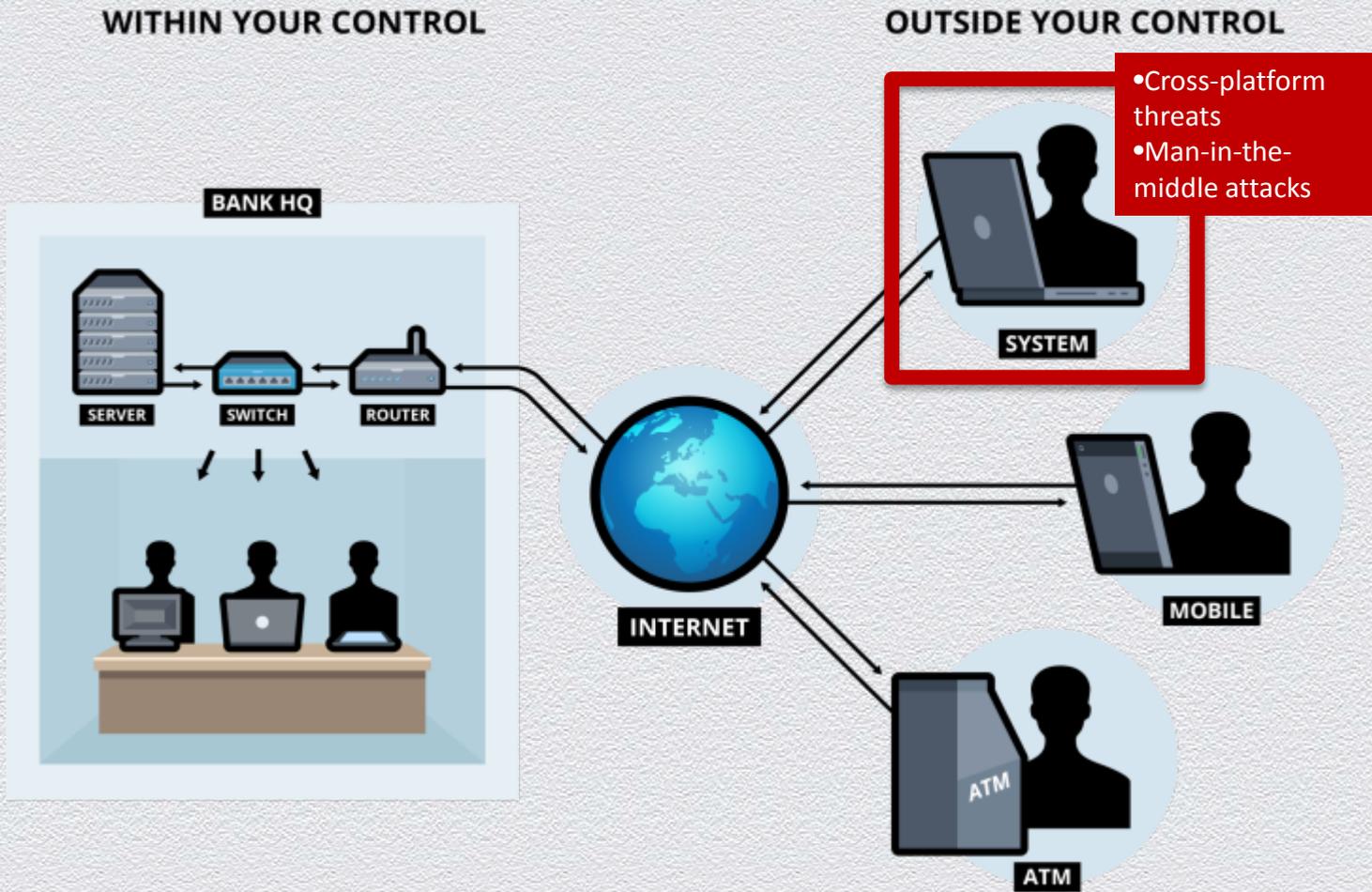
## Distribution of Mobile Phishing URLs

*More than 40% of mobile phishing sites target financial services*

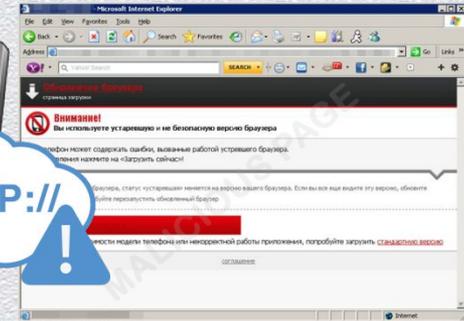
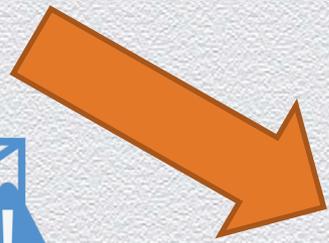
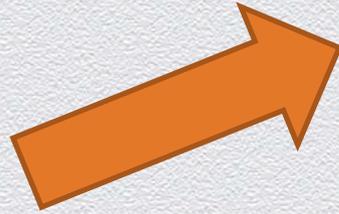
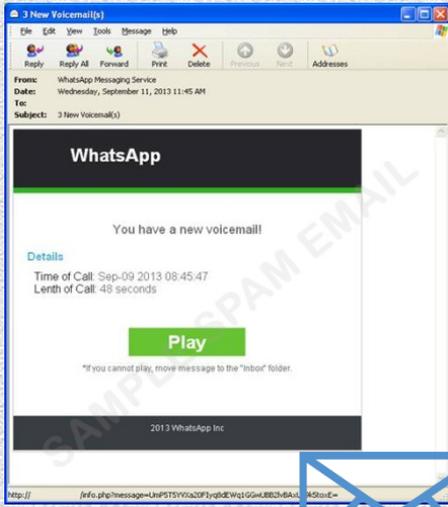
# Mobile Phishing



# Entry Points for Security Threats



# Cross-Platform Threats



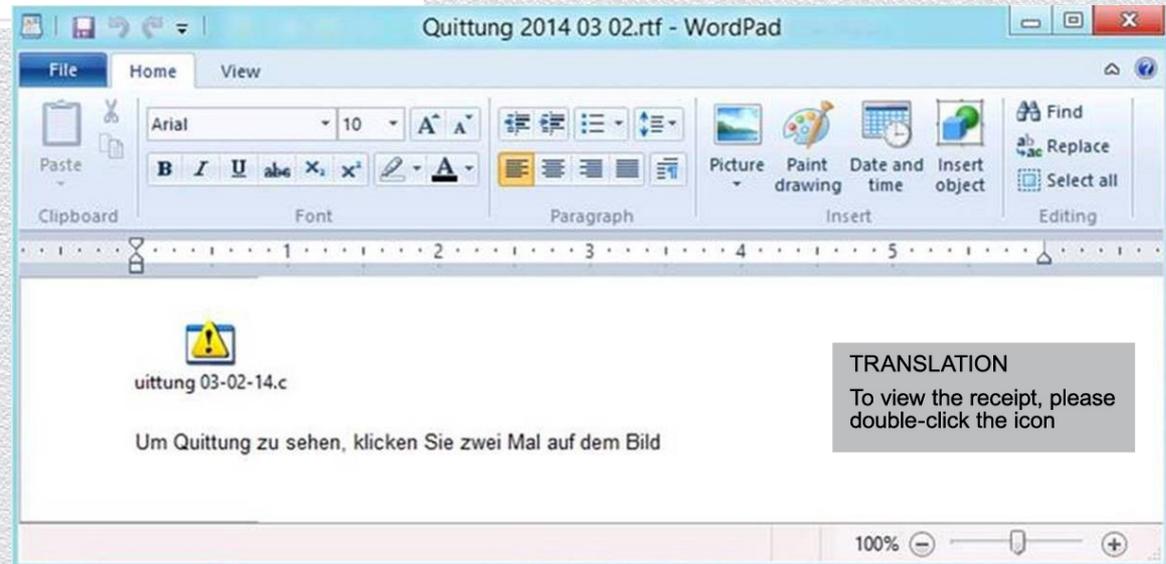
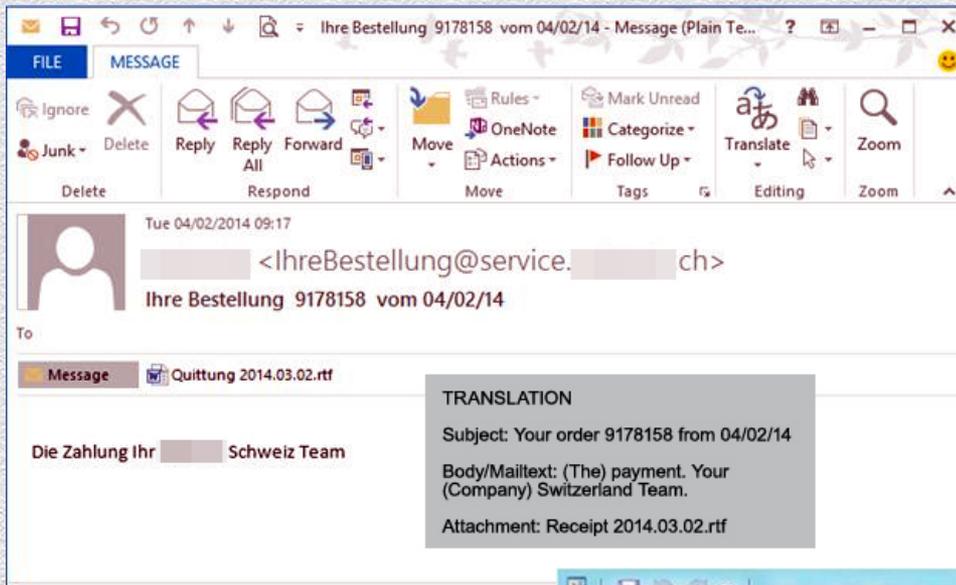
# Cross-Platform Threats



# Man-in-the-Middle Attacks



# Operation Emmental



# Operation Emmental

The screenshot shows a web browser window with the address bar containing "https://banking. [redacted] at". The browser's address bar includes navigation icons, a search engine (Google), and a home button. Below the address bar, there are several bookmarked folders: "Most Visited", "Release Notes", "Fedora Project", "Red Hat", and "Free Content".

The main content area of the browser displays a banking website. A modal window is open in the center, titled "Persönliche Identifikationsnummer" (Personal Identification Number). The modal contains the text "Bitte geben Sie Ihre PIN (Persönliche Identifikationsnummer) ein." (Please enter your PIN (Personal Identification Number)). Below this text is a text input field labeled "PIN:" with a cursor inside. A yellow "Anmelden" (Login) button is positioned below the input field.

The background website is partially obscured by the modal. Visible elements include a navigation menu with "Anmeldung" (Login), "Demo", "Hotline", and "Häufige Fragen (FAQ)". A section titled "Neu bei ELBA-internet?" (New to ELBA-internet?) contains the text "Fordern Sie Ihre Zugangsdaten an oder registrieren Sie sich gleich online." (Request your login data or register online) and a "Zugang anfordern" (Request access) button. There are also logos for "a-proved" and "Handelsverband".

Below the modal, the website shows a section for selecting a preferred login method: "Wählen Sie Ihr bevorzugtes Anmeldeverfahren:" (Select your preferred login method). There are three radio buttons: "Verfügernummer" (selected), "Benutzername" (Username), and "Digitale Signatur" (Digital Signature). Below this, there are input fields for "Bankleitzahl" (43672), "Konto oder Depot" (8991284242), and "Verfügernummer die letzten 8 Stellen" (ELOOE-01-V 89a9u239). A "Hilfe zur Anmeldung" (Help with login) link is also present.

# Operation Emmental

https://banking...at/#

Most Visited Release Notes Fedora Project Red Hat Free Content

English version

### Installierung der Mobileapplikation. Schritte 2.

1. Installieren Sie die mobile Applikation aus der SMS auf Ihrem Telefon und starten Sie es.
2. Dann werden Sie die Möglichkeit bekommen das Einmalpasswort für den Zugang zu Ihrem Konto zu generieren. Klicken Sie „Passwort generieren“ für die Generierung des Passwortes.
3. Geben Sie das erhaltene Passwort auf dieser Seite ein und klicken Sie auf 'Weiter'.

[Ich habe keine sms mit dem Link auf Mobilanlage erhalten.](#)

Einmaliges Passwort, das von der mobilen...  
eriert ist:

Weiter

Hilfe zur Anmeldung

Bitte geben Sie Ihre Bankleitzahl, Ihre Konto- oder Depotnummer sowie die letzten 8 Stellen Ihrer Verfügurnummer ein.

1-V 89a9u239

TRANSLATION

Installation process of the mobile app. Step 2.

1. Install the mobile app from the SMS on your phone and start it.
2. Then you will have the possibility to generate the one-time password for accessing your bank account. Click "Generate password" to generate a password.
3. Enter the displayed password on this page and click "Next."

I didn't receive an SMS with the link to the mobile app.

One-time password, generated by the mobile app:

# Operation Emmental

https://banking...at/#

Most Visited | Release Notes | Fedora Project | Red Hat | Free Content

English version

### Installierung der Mobile Applikation. Schritte 2.

1. Installieren Sie die mobile Applikation aus der SMS auf Ihrem Telefon und starten Sie es.
2. Dann werden Sie die Möglichkeit bekommen das Einmalpasswort für den Zugang zu Ihrem Konto zu generieren. Klicken Sie „Passwort generieren“ für die Generierung des Passwortes.
3. Geben Sie das erhaltene Passwort auf dieser Seite ein und klicken Sie auf Weiter.

Ich habe keine sms mit dem Link auf Mobilanlage erhalten.

Wenn Sie aus irgendwelchem Grund SMS mit dem Link auf Ihre Mobilanlage nicht erhalten können, nutzen Sie alternative Downloads-Varianten.

Geben Sie in Ihrem **Mobilbrowser** nächste Adresse ein:

229195

Weiter

ELOOE-01-V 89a9u239

die letzten 8 Stellen

Verfügernummer ein.

TRANSLATION

If you didn't receive the link to your mobile phone for whatever reason, please use alternative download methods:

Enter into your mobile browser the following address

hxxp://bit.do/kFCN

or scan the QR code.

# Operation Emmental



Den neuen Benutzungsvorschriften gemäß, soll jeder Versuch Ihr Bankkonto einzutreten mit Hilfe Einmalpasswort verwirklicht sein. Dieses Passwort können Sie mit Hilfe dieses Programm für Ihr Smartphone generieren. Drücken Sie „Passwort generieren“ auf und System wird Ihr Einmalpasswort generieren. Füllen Sie es in Ihrem Online-Banking ein, wenn es angefragt sein wird. Dieses Passwort ist nur für einen Versuch verfügbar. Deshalb löschen Sie dieses Programm nicht. Ohne es können Sie nicht Ihr Bankkonto benutzen.

Passwort generieren

© 

## TRANSLATION

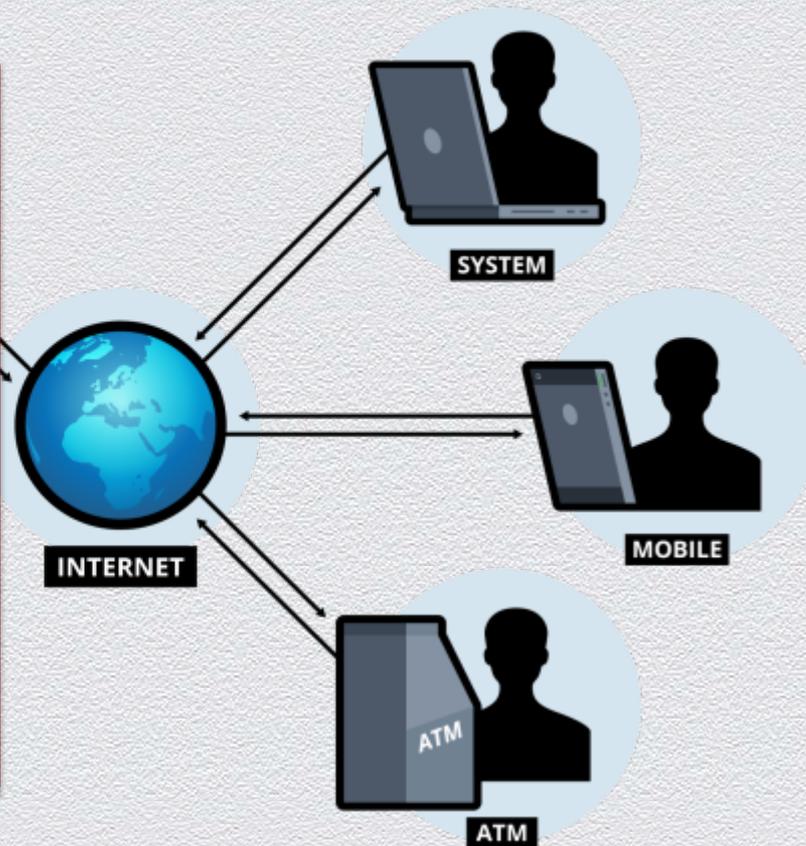
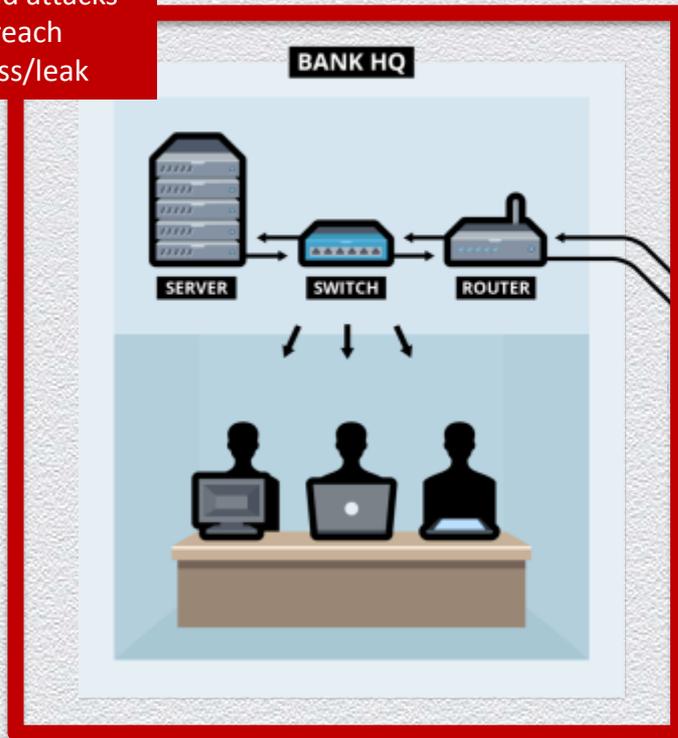
According to the new policy, for every attempt to log into your bank account a one time password is needed. This password can be generated with the help of this app on your smartphone. Click on "Generate password" to generate a password. Enter it into your online banking, if asked to do so. The password is only valid for one attempt. Therefore do not delete this app. Without this app you cannot use your online banking anymore.

# Entry Points for Security Threats

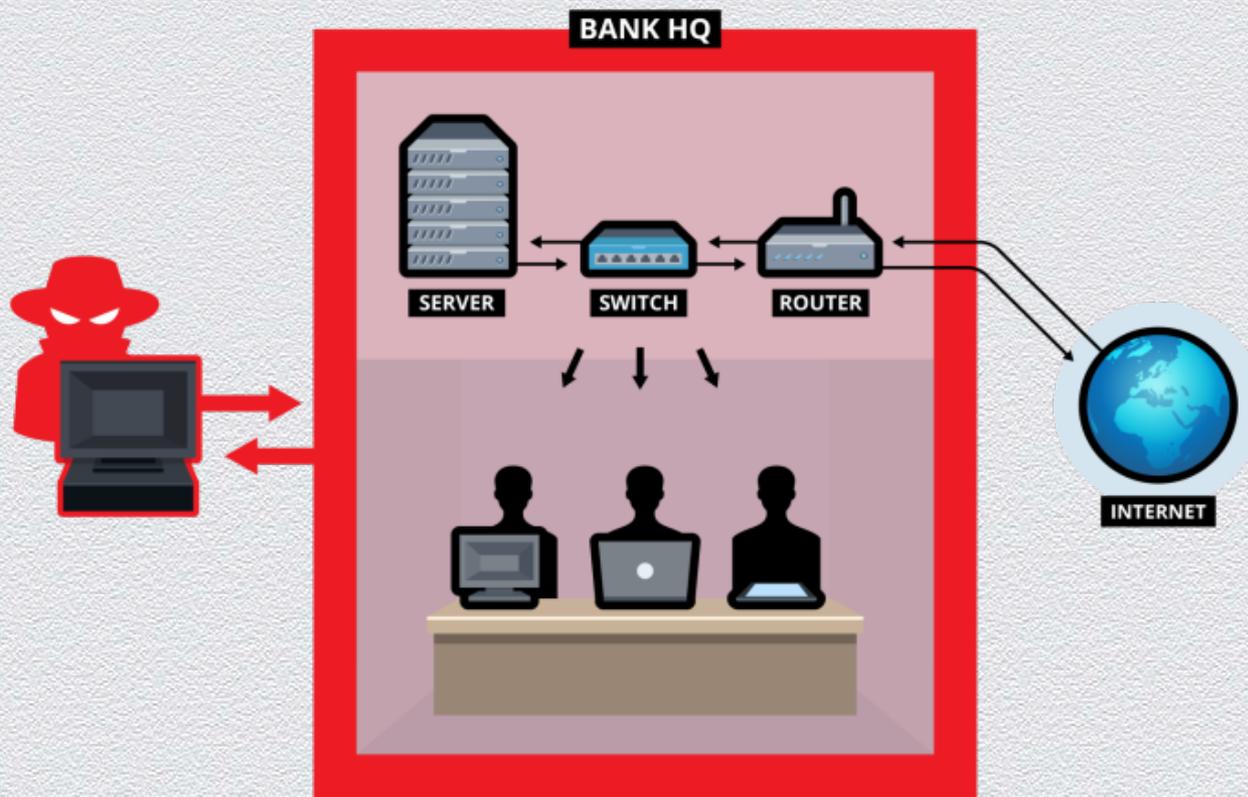
WITHIN YOUR CONTROL

OUTSIDE YOUR CONTROL

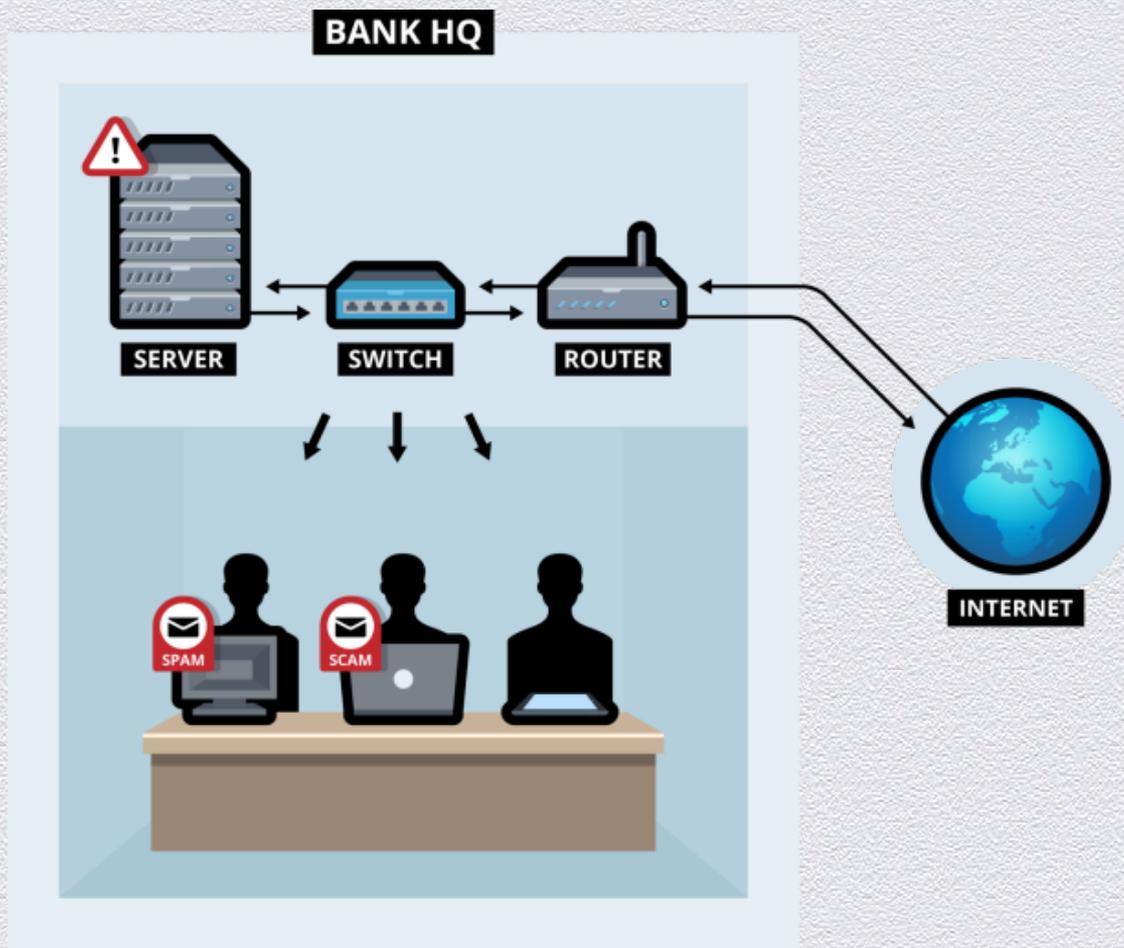
- Targeted attacks
- Data breach
- Data loss/leak



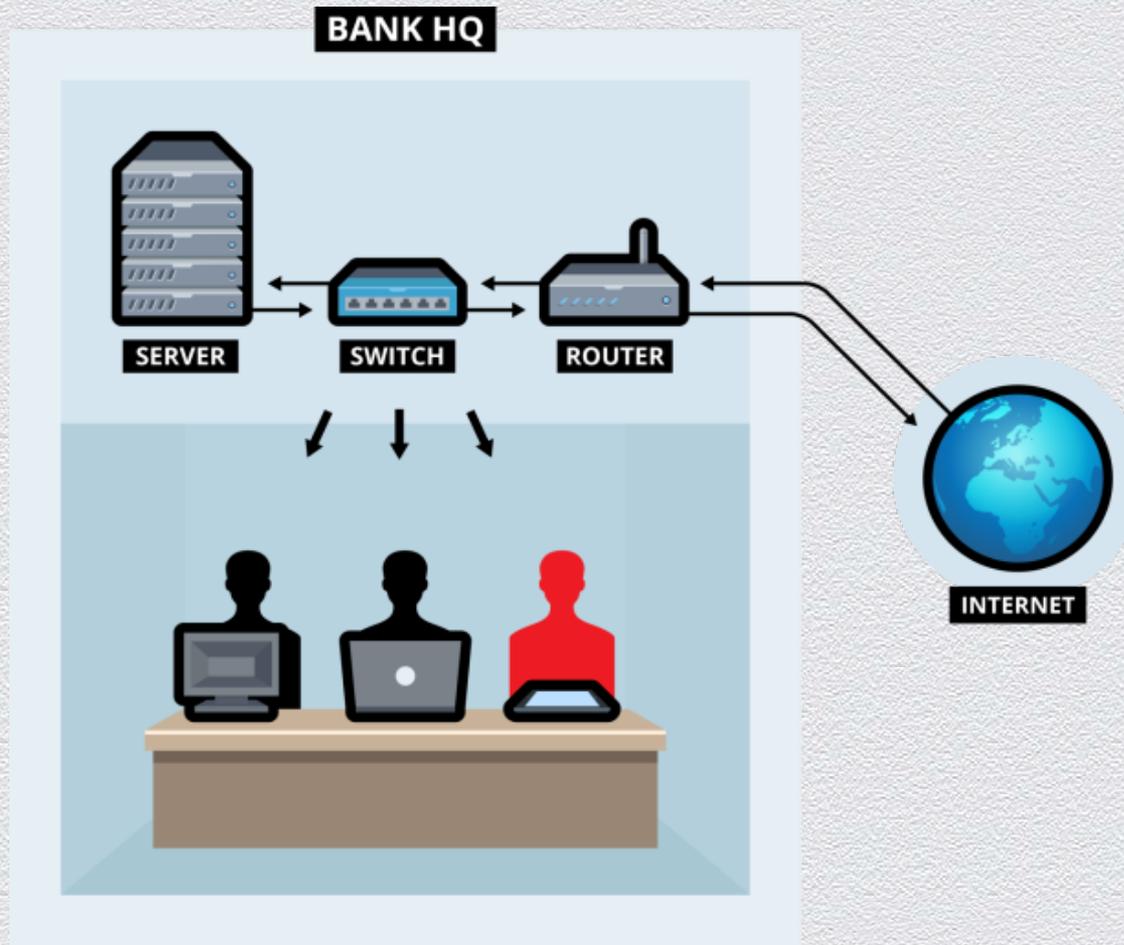
# Security Threats to Enterprises: Targeted Attacks



# Security Threats to Enterprises: Data Breach



# Security Threats to Enterprises: Data Leak/Loss



## VULNERABILITIES / THREATS

12/12/2013  
08:10 PM

# Weak Security In Most Mobile Banking Apps



Kelly Jackson  
Higgins  
News

**Eight of 10 iOS, Android mobile banking apps are improperly configured, new report says**

Most mobile banking apps -- including those of major financial institutions -- contain configuration and design weaknesses that leave them with weakened security.

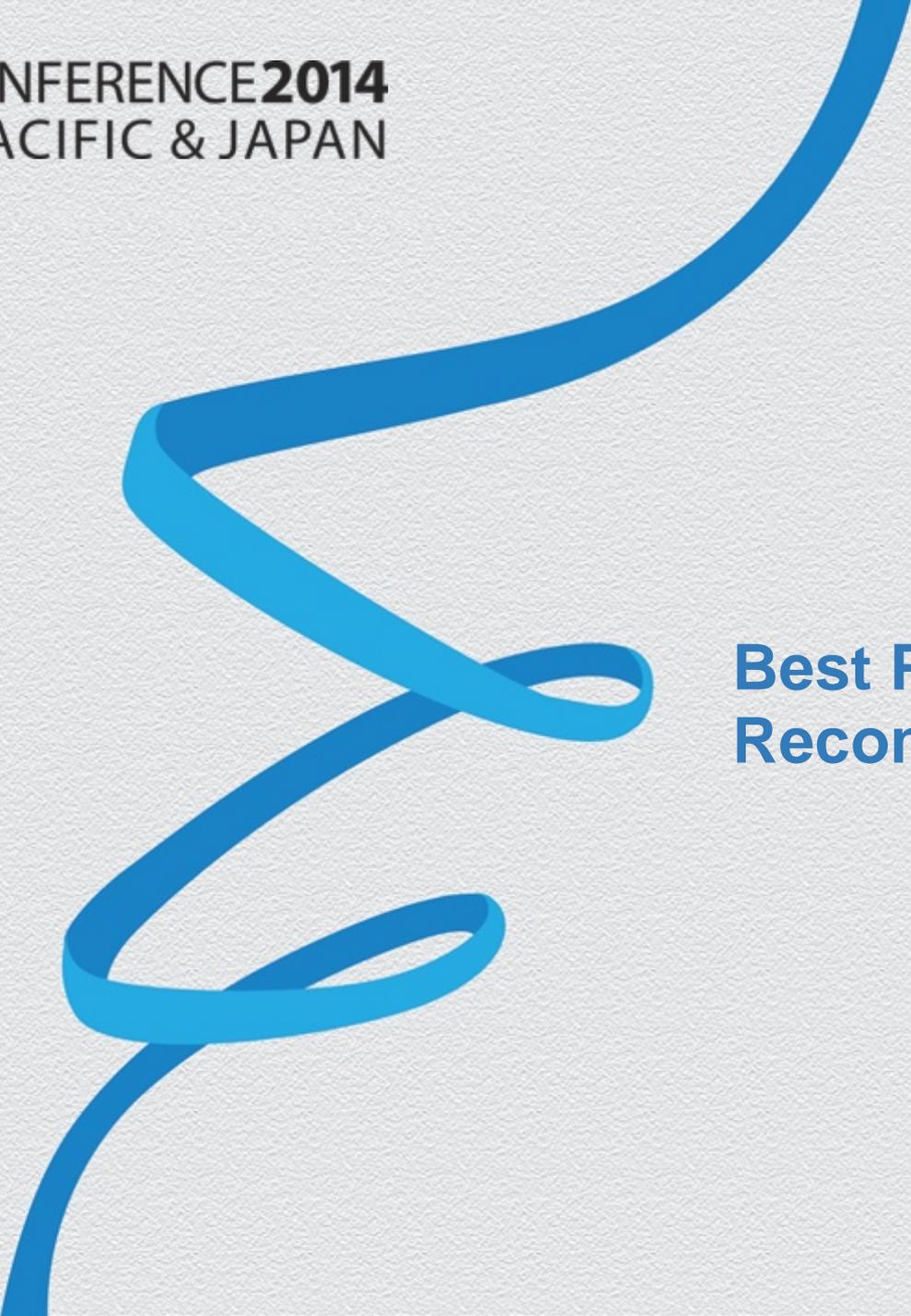
Connect Directly



0 COMMENTS

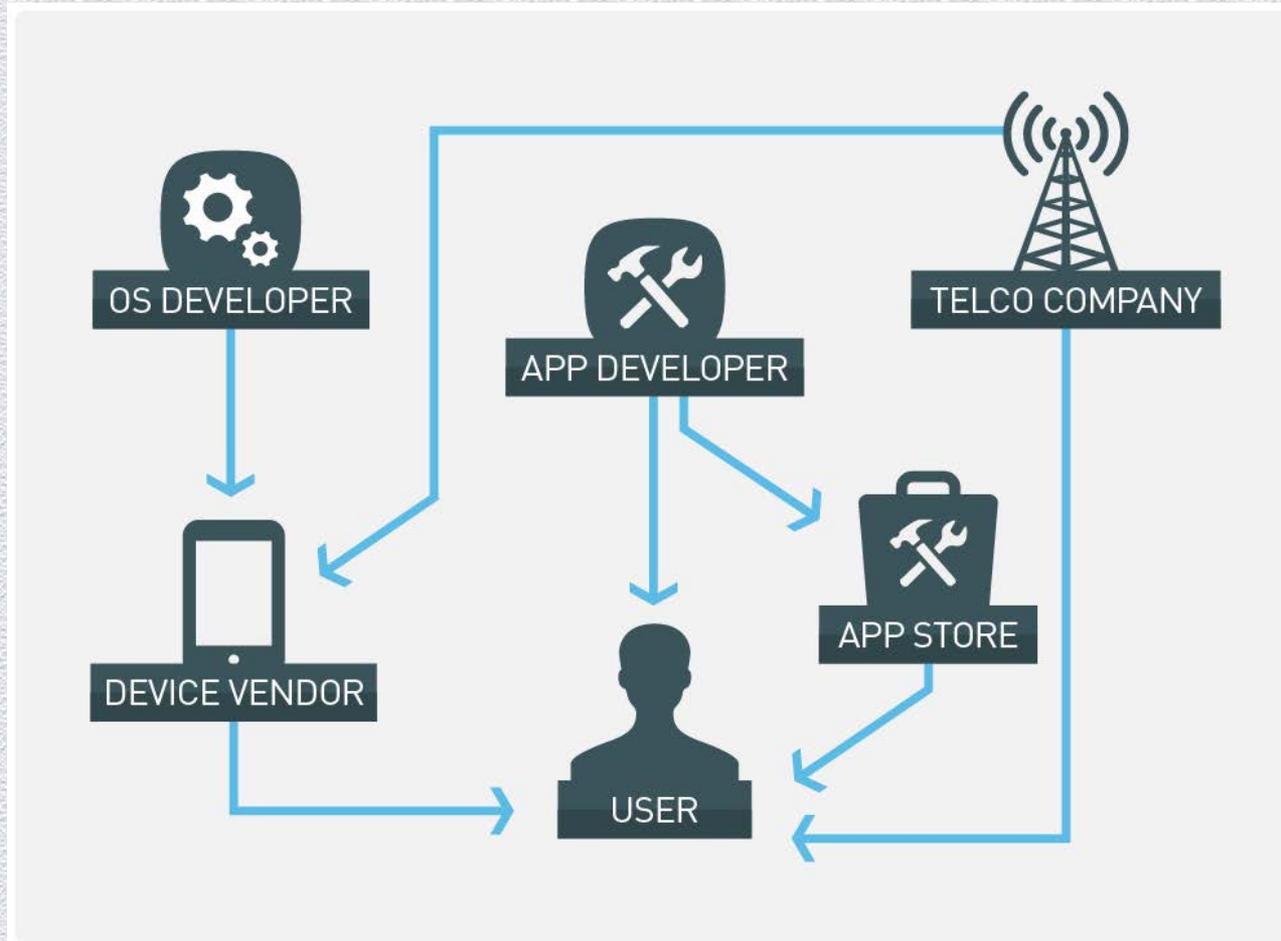
[COMMENT NOW](#)

Security experts this month tested 275 Apple iOS- and Android-based mobile banking apps from 50 major financial institutions, 50 large regional banks, and 50 large U.S. credit unions. Overall, they found that eight out of 10 apps were improperly configured and not built using best practices software development. Among the big-name banks whose mobile apps were tested by security firm Praetorian include Bank of America, Citigroup, Wells Fargo, Goldman Sachs, Morgan Stanley, Capital One Financial, and Suntrust Banks. Praetorian did not disclose how each bank's apps fared in the tests.

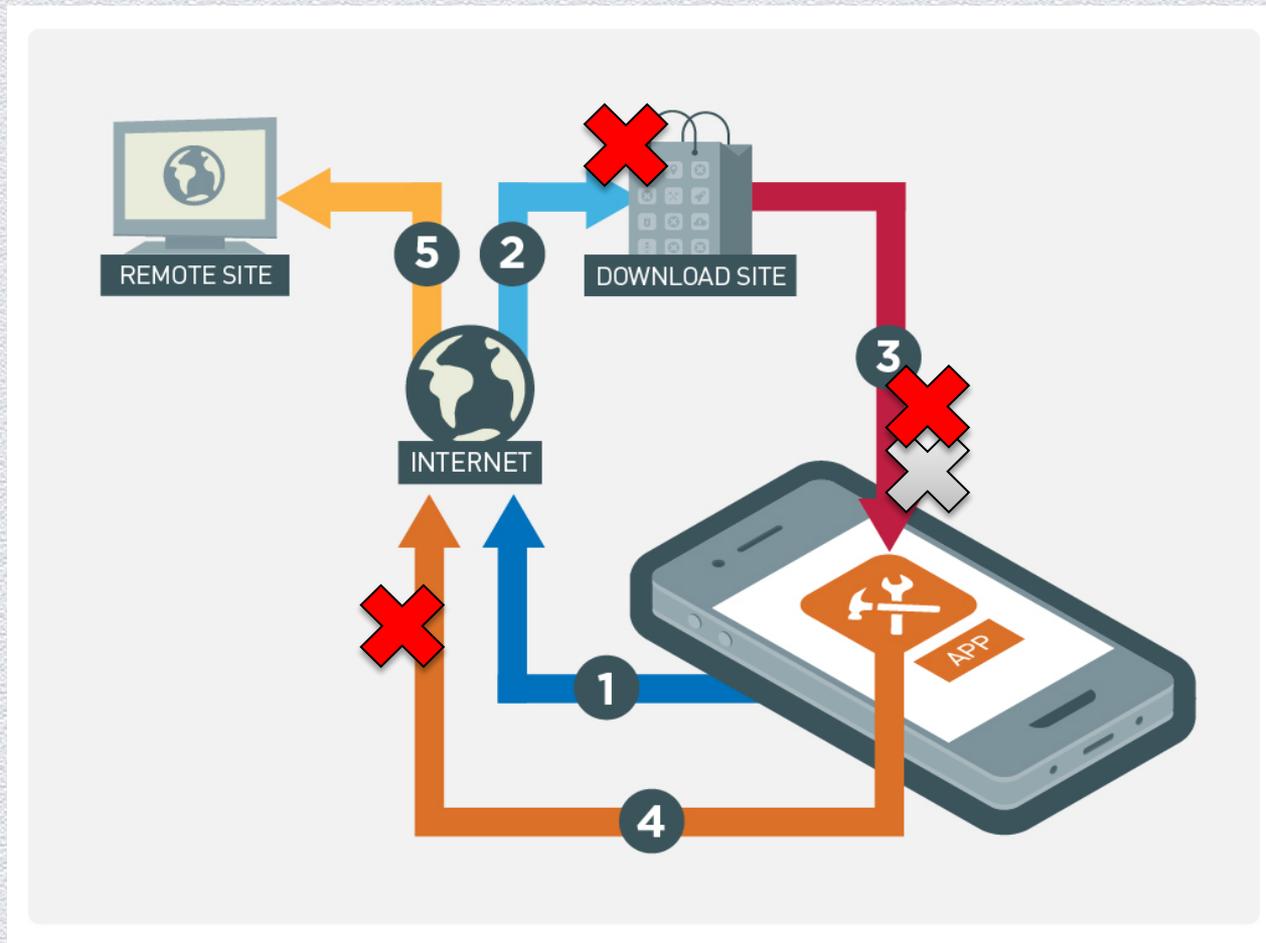


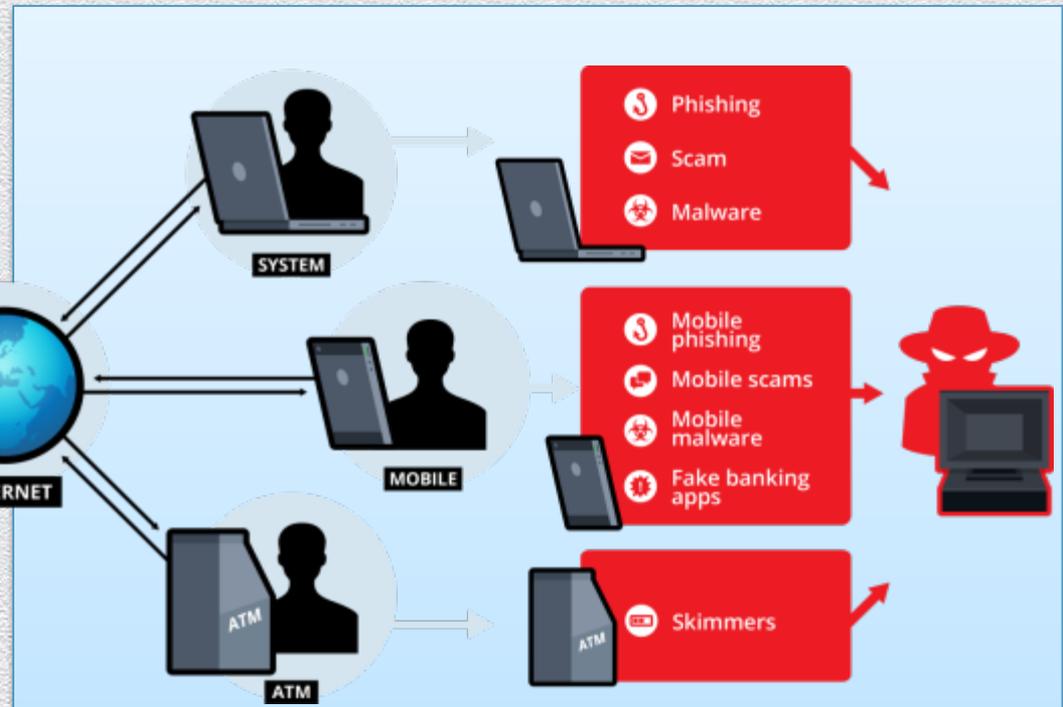
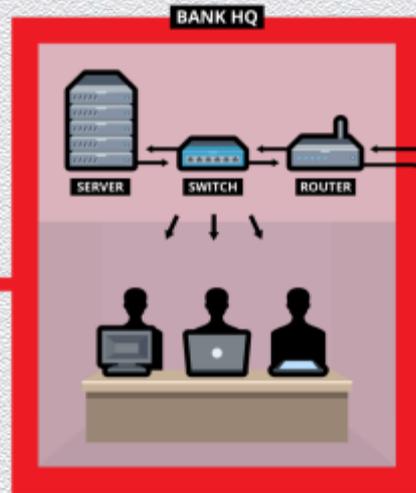
## Best Practices and Recommendations

# Securing the Mobile Ecosystem

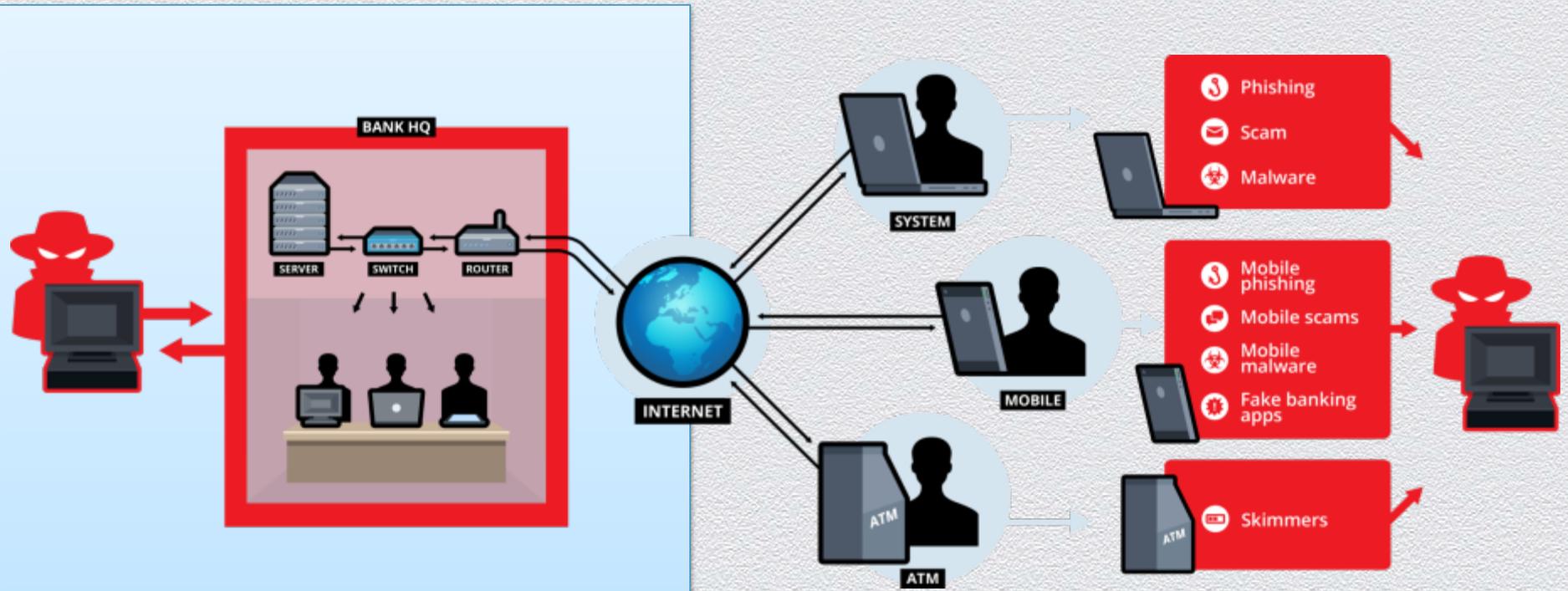


# Addressing Threats at the Exposure Layer





1. Customer Advisory:
  - Use of security software
  - Update/Patch systems
  - Social engineering watch
2. Two-Factor Authentication



1. Virtual Patching
2. Custom Defense
3. Employee awareness and education

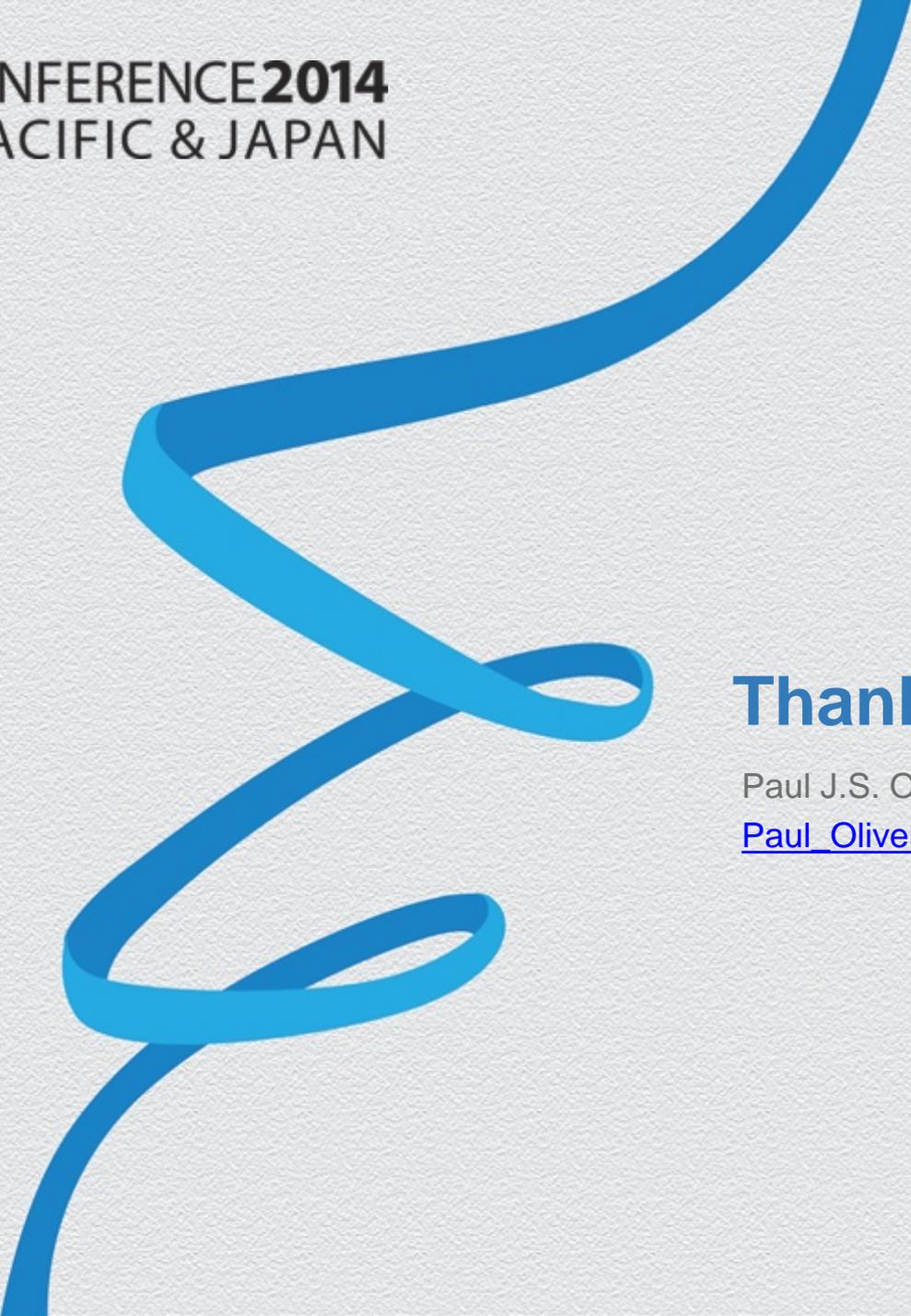
# Summary

- ◆ Everything is going mobile, including online banking cybercrime
- ◆ Online banking threats continue to evolve, and may even render “traditional” security measures useless
- ◆ Securing the mobile ecosystem against online banking threats needs to be a collaborative effort

A person wearing a white lab coat and glasses is looking at a tablet. The tablet screen displays a mobile banking application interface. The interface includes a header with 'MOBILE BANKING' and 'Account Information'. Below this, there are several sections: 'My Accounts' with a list of accounts, 'My Cards' with a list of cards, and 'TOTAL BALANCE' at the bottom. The background is a blurred indoor setting with a cup of coffee on a table.

If history is repeating, it's better to repeat the good side of it

**RSAC** CONFERENCE 2014  
ASIA PACIFIC & JAPAN



**Thank You!**

Paul J.S. Oliveria

[Paul\\_Oliveria@trendmicro.com](mailto:Paul_Oliveria@trendmicro.com)