

DECLARATION OF MINA CHING

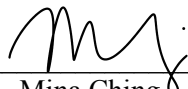
1. I am a Records Request Processor at the Internet Archive. I make this declaration of my own personal knowledge.
2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.
3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to browse more than 450 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a display of available dates. The visitor may select one of those dates, and begin browsing an archived version of the Web. Links on archived files in the Wayback Machine point to other archived files (whether HTML pages or other file types), if any are found for the URL indicated by a given link. For instance, the Wayback Machine is designed such that when a visitor clicks on a hyperlink on an archived page that points to another URL, the visitor will be served the archived file found for the hyperlink's URL with the closest available date to the initial file containing the hyperlink.
4. The archived data made viewable and browseable by the Wayback Machine is obtained by use of web archiving software that automatically stores copies of files available via the Internet, each file preserved as it existed at a particular point in time.
5. The Internet Archive assigns a URL on its site to the archived files in the format `http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL]` aka an "extended URL". Thus, the extended URL `http://web.archive.org/web/19970126045828/http://www.archive.org/` would be the URL for the record of the Internet Archive home page HTML file (`http://www.archive.org/`) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). The date indicated by an extended URL applies to a preserved instance of a file for a given URL, but not necessarily to any other files linked therein. Thus, in the case of a page constituted by a primary HTML file and other separate files (e.g., files with images, audio, multimedia, design elements, or other embedded content) linked within that primary HTML file, the primary HTML file and the other files will each have their own respective extended URLs and may not have been archived on the same dates.



archive.org

6. Attached hereto as Exhibit A are true and accurate copies of browser screenshots of the Internet Archive's records of the archived files for the URLs and the dates specified in the attached coversheet of each screenshot.
7. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

DATE: December 10, 2025



Mina Ching

EXHIBIT A

<https://web.archive.org/web/20130609185904/https://security.stackexchange.com/questions/36609/could-my-banks-two-factor-authentication-be-hacked>

INFORMATION SECURITY

Questions Tags Tour Users Ask Question

IT Security Stack Exchange is a question and answer site for IT security professionals. It's 100% free, no registration required.

Tell me more

Could my bank's two-factor authentication be hacked?

13
★
1

When I attempt to log in to my bank, an SMS code is sent to my phone. I then type this nine-character code into the bank's Web site, to login to my account.

Is this vulnerable to attack, without hacking the bank's software or server, or without access to my telephone/SMS communications?

How could it be exploited? So far, the only way I can imagine would be for someone to install an app on my phone which intercepts SMS traffic, and resends the code to an attacker. How could I prevent this from happening to me?

phone sms banks smartphone protection

share improve this question

edited Jun 4 at 21:21



Forest Monsen
11 ● 2

asked May 29 at 8:32



Derfder
146 ● 10

The [wikipedia article on TAN](#) also contains a section about security of SMS confirmation codes (section "Mobile TAN"). – [sleske](#) May 29 at 16:16

Yes they can 'cause of gsm. [ftp.ccc.de/congress/2012/mp4-h264-HQ/...](#) Start at minute 30. – [mic](#) Jun 4 at 19:33

2 Answers

active oldest votes

13

You are right in that one of the ways an attacker could intercept the code is to hack your phone. An attacker could also:

- Clone your phone's sim, and request a banking code to be sent to your phone's number. they could also possibly clone a non-sim phone as well
- Steal your phone. Once they have your phone they could perform transactions
- Perform a man in the middle attack when you use your banking site. This has been done already, an attacker uses malware installed on your computer to direct your banking traffic to a site set up to mimic your bank's page. When you type in the code the malware gets it, then uses the code to perform a transaction
- Social engineer your bank to change your mobile phone details to a phone they control. If an attacker knows enough about you, and your bank's procedures aren't tight enough, then the attacker could call your bank pretending to be you and get them to change the mobile number

So what can you do?

- Keep control of your mobile phone.
- Make sure your computer is kept up to date with patches and anti-malware software
- Do all your banking on a virtual machine, and never save its state. If your virtual machine gets hacked and you save the state then the malware will remain in the virtual machine, however if you never save its state the malware won't be able to remain on the virtual machine
- Many banks use some sort of authentication code to verify the identity of people calling. Write these down but do not put them onto your computer or phone, that way there's still something an attacker does not know, even if they have full access to your computer and your online identity.

It's not all doom and gloom, most of the time banks can reverse transactions if caught quickly, if you suspect that a fraudulent transaction has taken place get onto your bank ASAP and get their investigators on it. How well this may go depends on what the local laws are and how good your bank is.

share improve this answer

edited May 29 at 9:56

answered May 29 at 9:13



GdD
5,865 ● 5 ● 23

just curious to know what do you mean by work off a copy of VM every time. – [Ali Ahmad](#) May 29 at 9:48

When you create a VM for security purposes make a copy of it and use the copy. That way if you accidentally save its state you can make another copy from the master. I didn't mean make a fresh copy every time you bank. You're right, it was confusing, I'll edit. – [GdD](#) May 29 at 9:54

Thanks for the info and ideas. It's definitely a good idea to use Virtual machine with some Debian or something just for accessing bank accounts ;). – [Derfder](#) May 29 at 10:03

Using a VM from an infected computer is not very secure is it? I guess having a clean base system that you don't use for anything (except updating) and then on top a different VM for every task you perform would be

tagged

phone × 41

sms × 24

banks × 14

smartphone × 12

protection × 5

asked 11 days ago

viewed 538 times

active 4 days ago

Related

- 4 How can I protect my phone voicemail from being hacked?
- 27 How hard is it to intercept SMS (two-factor authentication)?
- 3 SMS / voice call interception with a fake base station
- 5 Proof of SIM card possession on iOS devices
- 1 What's the deal with SMS archiving?
- 10 How does HSBC's "Secure Key" actually work?
- 1 Can 2FA help handle mixed personal and business accounts after leaving a company?
- 3 What security factors should I take into consideration when selecting a bank?
- 6 How is Chase Mobile Deposit Secure?
- 2 Is TextKey SMS 2 factor authentication secure against cell phone cloning?

@OmarKohl, I'd say that's a given, it's still more secure than using the base machine for your transactions though. The point in using a VM would be to help keep your system from getting compromised in the first place. – GdD May 29 at 15:33

7

Second factor authentication was designed and used properly in the past but lately it has been weakened by companies who care more about profit than security. SMS messages cannot recreate the security level of carefully designed RSA tokens and smart cards.

[Cloning the SIM card](#) can be much easier when social engineering enters the picture. Cloning is still hard and cannot scale like [SMS interception](#) can. And you don't need to build your own cracking system, you can buy it in [big](#) or [small](#) packs.

An old method is called [SIM card partitioning](#) and is a side-channel attack method that pulls key data from SIM cards by monitoring side channels such as power consumption and electromagnetic emanations. The technique requires some physical proximity and can extract secret cryptographic keys in minutes. Previously, an attacker would need access to a SIM card for at least eight hours to carry out a successful attack.

Protect against these by first educating yourself about threats and good security practices. A checklist of things to do can protect against common pitfalls, but having a security mindset will get you further.

edited Jun 4 at 20:58

answered May 29 at 9:42



Cristian Dobre

3,960 1 7 29

An old method is called SIM card partitioning and is a side-channel attack methodology that pulls key data from SIM cards by monitoring side channels such as power consumption and electromagnetic emanations. The technique can extract secret cryptographic keys in minutes. Previously an attacker would need access to a SIM card for at least eight hours to carry out a successful attack.

cs.washington.edu/research/projects/poirot3/Oakland/sp/PAPERS/... – Cristian Dobre May 29 at 13:22

In the past, attackers used information from a phone company insider to clone SIMs and commit banking fraud. There is a very recent wave of SIM swap fraud in South Africa where attackers trick the phone company into giving them a new SIM card. – [Cristian Dobre](#) May 29 at 15:23

show 3 more comments

B *I*

 Sign up using Google

 Sign up using Facebook

Name	<input type="text"/>
Email	<input type="text"/>

 Sign up using Stack Exchange

Post Your Answer

By posting your answer, you agree to the [privacy policy](#) and [terms of service](#).

Not the answer you're looking for? Browse other questions tagged [phone](#) [sms](#) [banks](#) [smartphone](#) [protection](#) or [ask your own question](#).

 question feed

[about](#) [help](#) [badges](#) [blog](#) [chat](#) [data](#) [legal](#) [privacy policy](#) [jobs](#) [advertising info](#) [mobile](#) [contact us](#) [feedback](#)

TECHNOLOGY			LIFE / ARTS	CULTURE / RECREATION	SCIENCE	OTHER
Stack Overflow	Programmers	Database Administrators	Photography	English Language & Usage	Mathematics	Stack Apps
Server Fault	Unix & Linux	Drupal Answers	Science Fiction & Fantasy	Skeptics	Cross Validated (stats)	Meta Stack Overflow
Super User	Ask Different (Apple)	SharePoint	Seasoned Advice (cooking)	Mi Yodeya (Judaism)	Theoretical Computer Science	Area 51
Web Applications	WordPress Answers	User Experience	Home Improvement	Travel	Physics	Stack Overflow Careers
Ask Ubuntu	Geographic Information Systems	Mathematica	more (13)	Christianity	more (7)	
Webmasters	Electrical Engineering			Arqade (gaming)		
Game Development	Android Enthusiasts			Bicycles		
TeX - LaTeX	IT Security			Role-playing Games		
				more (21)		

site design / logo © 2013 stack exchange inc; user contributions licensed under cc-wiki with attribution required
rev 2013.6.9.131