

The Wayback Machine - <https://web.archive.org/web/20130609185904/http://security.stackexchange.com:80/questions/36609/could-my-banks-two-factor-authenticat...>

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?

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](#)

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/...](ftp.ccc.de/congress/2012/mp4-h264-HQ/) Start at minute 30. – [mic](#) Jun 4 at 19:33

2 Answers

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.

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 perfect (but cumbersome). – [Omar Kohl](#) May 29 at 14:47

@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

The whole idea about a second factor/step for authentication is to provide two independent layers of security. Vulnerabilities in one layer should not affect the security of the other.

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.

Attacks on SMS as second factor are no longer theoretical but multi-million dollar crimes. Compromising the phone is the most strait forward approach and was used at least in this [47 million dollar heist](#).

[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.

And just when you think the second factor is secure and you can rely on it, consider the [man-in-the-browser type of attack](#).

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.

In the past, attackers used information from phone company insiders to clone SIMs and then commit banking fraud. Currently, there is a wave of [SIM swap fraud](#) in South Africa where attackers trick the phone company into giving them a new SIM card.

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



[Forest Monsen](#)
11 2

answered May 29 at 9:42



[Cristian Dobre](#)
3,960 1 7 29

thanks, but what do you mean by cloning a SIM card? Could it be done without having the physical copy of my SIM card in the hacker hands? I guess not. Or am I wrong? – [Derfder](#) May 29 at 10:01

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

Thanks, so he needs to physically examine the sim card? We are talking about crackers not some cia/nasa "ufo" experimental technologies. Basically I want to know if somebody can clone my sim card without actually having it in their hands, e.g. by downloading something from my phone via some malware or something like that. Or this way it cannot be done. – [Derfder](#) May 29 at 13:30

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

10/17/25, 5:46 PM

phone - Could my bank's two-factor authentication be hacked? - IT Security Stack Exchange

new SIM card. – [Cristian Dobre](#) May 29 at 15:23

Thanks, so downloading some info from my cell phone via a virus or some malware is not enough to clone a SIM card? – [Derfder](#) May 29 at 15:57 