

WHITE PAPER

The Hidden Dangers of SMS OTP: Why It is Time to Rethink Your Security Strategy

The Hidden Dangers of SMS OTP: Why It is Time to Rethink Your Security Strategy

TABLE OF CONTENTS

Regulation and Industry Changes

- [Man-in-the-Browser Attack](#)
- [SMS Malicious Number Porting/SIM Swapping](#)
- [SS7 Hacks](#)
- [SMS Marketing/Enablement](#)
- [SMS Interception: Rogue Cell Towers](#)
- [SMS Mobile Malware](#)
- [Online Access to SMS Messages](#)
- [SMS Phishing/Social Engineering](#)

SMS Delivery Issues

The heavy use of Short Message Service (SMS) as a long-term authenticator is concerning. SMS has long been regarded as a *less secure* form of multi-factor authentication, and it was even being considered for deprecation by the National Institute of Standards and Technology (NIST). While SMS was upheld by the revised Payment Services Directive 2 (PSD2) and Payment Services Directive 3 (PSD3), it has received heavy criticism. There are major weaknesses specifically associated with SMS. While SMS remains popular because of its prevalence, SMS faces significant security challenges.

Regulation and Industry Changes

November 2012: Australian Telcos declare SMS unsafe for bank transactions

June 2016: The NIST initially announced deprecation of SMS and published a [blog](#) about it. The organization later revised this position because of the lack of broad two-factor authentication use in general ([discussion](#)). The NIST text is shown in the following section.

5.1.3.2. Out of Band Verifiers

Out of band verifiers shall generate a random authentication secret with at least 20 bits of entropy using an approved random number generator. They then optionally signal the device containing the subscriber's authenticator to indicate readiness to authenticate. If the out of band verification is to be made using an SMS message on a public mobile telephone network, the verifier shall verify that the pre-registered telephone number being used is actually associated with a mobile network and not with a VoIP (or other software-based) service. It then sends the SMS message to the pre-registered telephone number. Changing the pre-registered telephone number shall not be possible without two-factor authentication at the time of the change. OOB using SMS is deprecated and will no longer be allowed in future releases of this guidance.

October 2017: Payment Card Industry 3-D Secure (PCI 3DS)

While SMS is not specifically called out (section 5.3 on authentication is very sparse), the unencrypted nature of its transmission appears to prohibit its use in section 5.2.3 of the [PCI 3DS standard](#).

5.2.3 Controls are implemented to protect the confidentiality and integrity of accounts and credentials.

*Implementation Guidance: “Implemented controls should protect the confidentiality and integrity of accounts for both local and remote users. The controls should include ensuring that **account and credential information is securely transmitted and stored—for example, using cryptography—at all times.**”*

May 2018: PSD2 (applicable throughout the European Union) provides for [limited use](#) of SMS, but even this use is under scrutiny. PSD2 requires that “payment service providers shall ensure the confidentiality and integrity of the personalized security credentials of the payment service user, including authentication codes, during all phases of the authentication”, something not possible on the unencrypted public switched telephone network.

February 2023, Twitter: https://blog.x.com/en_us/topics/product/2023/an-update-on-two-factor-authentication-using-sms-on-twitter

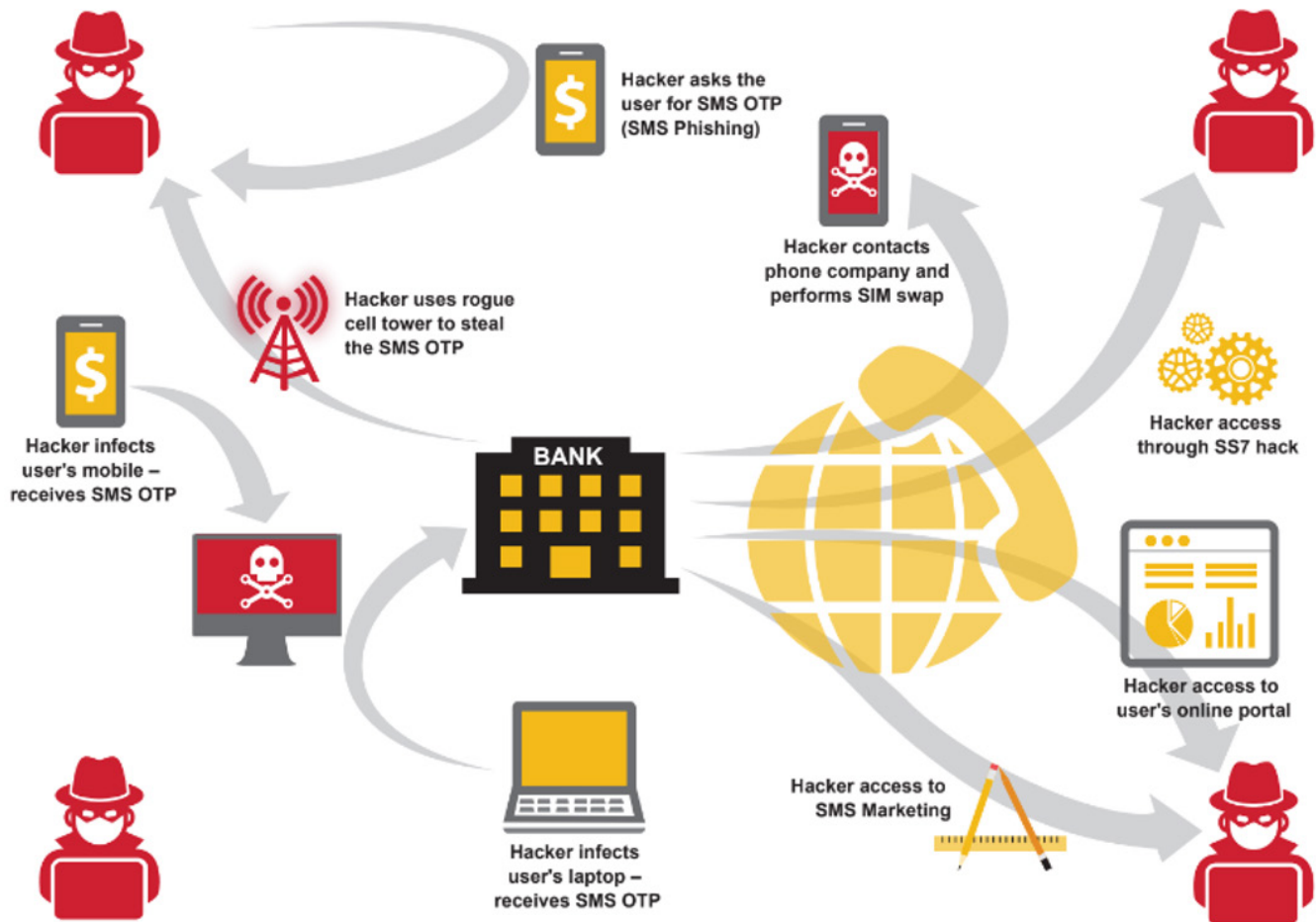
September 2023, Microsoft: <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-system-preferred-multifactor-authentication>

2024: PSD3 increases the mention of strong customer authentication (SCA) as it seeks to apply SCA to more places. Discussion is ongoing for the Regulatory Technical Standards (RTS). These rules will define the technical criteria of what constitutes *strong customer authentication* or not—including whether SMS will be in-scope or out-of-scope.

February 2024, Oracle: <https://community.oracle.com/netsuite/english/discussion/4491361/final-reminder-end-of-support-for-two-factor-authentication-by-sms-voice-call>

April 2024: The NIST [acknowledges](#) that SMS is less secure. “Attestations *should not* be used for broad public-facing applications. Such a requirement ... may divert users to less secure authentication options that are vulnerable to phishing, such as Short Message Service (SMS).”

This graphic summarizes the various methods by which SMS OTP can be stolen. Each is discussed in the following sections



Man-in-the-Browser Attack

Cost: Malware creation, distribution, and server maintenance

Dyre [malware](#) was crafted to target a user's normal bank access to take over the user's account.

In this situation, malware has taken over a computer and waits for the user to access a particular bank website. The following events occur:

1. The user accesses their bank and the malware hijacks this access.
2. Malware changes the request to go to a malicious server.
3. The request is delivered to the malicious server.
4. The malicious server sends a look-alike login page to the user.
5. The user supplies genuine credentials to the malicious server, including SMS one-time password (OTP).
6. The malicious operator takes over the victim's account.

SMS Malicious Number Porting/SIM Swapping

Cost: Social engineering

The temporary nature of individual cell phones, cell phone components, and even the ability to save your phone number but switch mobile providers provides ease of use, but also provides an avenue for fraudsters to steal your phone number. The essence of a phone number is the tie between that number and a specific hardware component, the International Mobile Subscriber Identity (IMSI). The IMSI number is physically associated with the subscriber identity module (SIM) card. The SIM card is what identifies this specific phone to the phone network. When switching phones, the new SIM is needed to know which physical phone to associate with the subscriber's phone number so the user's service can continue.

To perform this attack, a scammer performs the following actions:

1. Contact the mobile provider and convince them that they are the victim. If they can socially engineer the identity validation protections that the mobile provider has in place, then they can port a target's phone to one that the scammer controls.
2. The scammer can then proceed to login to a target portal with the user's stolen username and password.
3. The scammer receives the victim's SMS OTP.
4. The scammer then accesses the victim's account.

SS7 Hacks

Cost: ~1000 Euros

Hackers can take advantage of the lack of authentication in an underlying phone network protocol, Signaling System 7 (SS7). The hackers use the protocol to redirect text messages to a number of their choosing. The necessarily open and unauthenticated nature of SS7 leaves it open to this type of abuse. This hack is discussed in some detail on the [Schneier on Security blog](#).

A hacker needs a target username, password, and phone number. To conduct this attack, the hacker performs the following steps:

1. Registers as a router on the public network using SS7
2. Request that messages for the user's handset should be routed to the attacker's router
3. Initiates a fraudulent login and receives the user's SMS OTP
4. Completes the login using the SMS OTP
5. Accesses the target's account

SMS Marketing/Enablement

Cost: \$25

Marketing needs have pushed providers to offer mass/automated SMS systems. These systems can send messages to many individuals at once. One system needs a *letter of authorization* to act as your phone, which allows it to receive that phone's texts and correspondingly send texts to many at once. This service costs \$25 at the time of this writing. This technique was examined in detail and demonstrated in real-time using a system called Sakari in an article on [Krebs on Security](#). This system can be used to steal a user's text messages without their knowledge or permission.

The following events occur:

1. A fraudster subscribes to Sakari and pays \$25.
2. The fraudster then supplies the target's phone number.
3. Sakari takes control of this phone number to enable it for high-volume marketing.
4. The fraudster attempts to login with the target's username and password.
5. The fraudster receives the user's SMS OTP.
6. The fraudster uses this password to complete a login as the user.
7. The fraudster accesses the target's account.

SMS Interception: Rogue Cell Towers

Cost: ~\$1500

Harris Corporation's *StingRay* device and *KingFish* device popularized the ability to track or intercept cellphone use. The devices either listen to active conversations or act as a cell tower and intercept all communications to handsets in a given area. While the primary customer base appears to be the military, the intelligence community, and law enforcement—the technique is not limited to the Harris Corporation. [Chris Paget](#) demonstrated this technique with a home-grown solution at Def Con 18.

This attack would begin with a hacker identifying a target username, password, and physical location. To conduct this attack, the hacker performs the following steps:

1. The hacker moves to a location frequented by the victim.
2. The hacker waits until the target's phone is in range.
3. The hacker activates the rogue cell tower and waits for the target's device to *join* this cell tower.
4. The hacker initiates a fraudulent login.
5. The hacker intercepts the target's SMS OTP and uses this information to complete a login as the victim. The target does not receive the SMS and is unaware their account is being attacked.
6. The hacker accesses the target's account.
7. The hacker can power down the rogue cell tower and cell devices, and then shift to other available cell towers in the area.

SMS Mobile Malware

Cost: Server operation cost, and Eurograbber malware production and distribution

Cybercriminals and other threat actors continue to find innovative ways to steal, defraud, and disrupt ordinary operations. Mobile devices are not exempt, and these devices have had many examples of malware for these platforms. In 2012, the [Eurograbber banking trojan](#) infected Android, Symbian, and Blackberry devices. The trojan then performed fraudulent money transfers during users' banking sessions. The following events occur:

1. The user's device is infected with Eurograbber.
2. The user browses to their bank on their mobile device.
3. The user successfully logs in to their bank.
4. Eurograbber initiates a bank transfer from the victim's account to a mule account.
5. The bank sends an SMS OTP to confirm the transaction.
6. Eurograbber intercepts this message and sends it to an attacker-controlled server.
7. The malicious server completes the authentication.
8. The fraudulent bank transfer is approved.

Online Access to SMS Messages

Cost: Zero

Some phone service providers offer an online portal to read SMS messages. Hackers that can login can have access to these messages and use these messages to login fraudulently to a website. Multiple providers offer the ability to see and send SMS messages from an online portal ([Verizon](#), [AT&T](#), [T-Mobile \(Sprint\)](#), and [Google](#)). An attacker able to breach the login for any of these portals can read and send SMS messages as a target from anywhere.

An attacker needs the user's username, password, and mobile number to begin. The attacker performs the following steps:

1. Breaches one of these online portals as the victim user
2. Initiates a fraudulent login as the victim user
3. Accesses the victim's SMS OTP through the online portal
4. Takes control of the victim user's account

SMS Phishing/Social Engineering

Cost: Zero

Phishing or social engineering, as applied to SMS targets users' lack of experience with authentication systems to contribute to a phisher's login attempts.

The phisher first collects the victim's username, phone number, and minimum account recovery details. The phisher then performs the following actions:

1. Logs in with stolen recovery information. The portal sends an OTP to the user.
2. The phisher sends their own SMS message to the user. The phishing text is similar to the following message: "We have detected a rogue sign-in to your <username> account. In order to determine the legitimate login we are going to send a verification code to your previously registered phone number from another support number. Please re-type the sent verification code in response to this message or your account will be permanently locked."
3. Users failing this phish will send the OTP back to the phisher.
4. The phisher then logs in and takes control of the account.

SMS Delivery Issues

Another issue affecting the service availability of OTP through SMS is network reliability. Once an OTP is triggered in Symantec® VIP, we deliver this to our vendor in only 20 ms. The vendor initiates the SMS message through one of its carrier links, but carrier outages, local tower operator outages, and other network issues delay the arrival of an SMS message—sometimes by several minutes.. Cell towers do not have perfect coverage, and a lack of handset reception can prevent SMS messages from being delivered. On a broader scale, countries can also block SMS messages. Each country can set its own rules. The following sections describe specific points of unreliability with SMS delivery. All of these points negatively contribute to lack of reliability with SMS delivery.

Countrywide Blocking

Each country can choose what SMS features to allow on its networks and whether to require any compliance in SMS messages. Some automatic blocking will also sweep up SMS OTP messages. China has [specific and detailed compliance](#)—effort is needed to prevent automatic blocking.

Carrier-to-Carrier Disruptions

Regional carriers either use their own equipment or link through local carriers that provide coverage for a specific geography. When the link between a regional carrier and a local carrier is lost, SMS messages cannot be delivered or are significantly delayed to the end customers in that area.

Local Carrier Outages

Access to the user's handset goes through the local cell tower. These cell towers are frequently managed by a local cellular company that contracts with one of the major provider networks (Verizon, AT&T, T-Mobile, and Boost Mobile). On the customer side, many smaller mobile virtual network operators (MVNOs) provide alternate options but still run on one of these major networks. On the delivery side, there are many [mobile network operators](#)—with smaller ones covering [specific geographies](#).

If a regional provider sends an SMS message to a local provider for delivery to the end subscriber, and that local provider is offline or having local technical difficulties, the OTP will not get through.

Lack of Cell Service Coverage

Cell service has [good coverage](#) in many metropolitan areas, but it is not universal. Complicating matters, 5G is more prone to being weakened by [ordinary construction materials](#). Just being inside a building that happens to be further from a cell tower may obstruct the signal to the cell tower and prevent communication.

SMS Engineered for Best Effort Delivery Expectation

Carriers do not offer a delivery guarantee for SMS traffic. Traffic is sent on a best-effort basis. Network congestion, traffic engineering, vandalism, voice and other critical traffic, and myriad other network challenges, all factor to negatively affect SMS delivery. When issues occur in the network, SMS is one of the first traffic loads to be abandoned while network stability is re-established. While the negative consequences of not receiving the latest marketing text message are likely minimal, not receiving an SMS OTP means that the user is stuck at a login screen. This translates to wasted time for the user.

Delivery Latency

Separately, delivery latency is not guaranteed. While a few seconds may be the norm, network issues do cause this to fluctuate up to several minutes—[long past the patience](#) of most users and past the login timers for some systems (30 to 60 seconds).