# Two-factor inauthentication – the rise in SMS phishing attacks


Markus Jakobsson

**Markus Jakobsson, Agari**

**There are countless ways to carry out a cyber-attack, but in the vast majority the key is deception – typically involving identity deception in which the attacker poses as a trusted party to the intended victim. Many of these attacks involve stealing passwords from victims in order to access their accounts and pose as them. Therefore, with cyber-criminals constantly on the prowl to capture passwords and other credentials, two-factor authentication (2FA) has become one of the most widely accepted back-up verifications for many services and companies.**

While various 2FA methods are available, the humble SMS text message has emerged as a favourite as it is incredibly ubiquitous and easy to understand. Whether it's a teenager armed with an iPhone X or a pensioner with an old Nokia 3310, all mobile devices support SMS and even the most inexperienced or technophobic user can read a text message.

Nevertheless, SMS also contains a number of inherent flaws as a security verification method. Whereas the SS7 vulnerability got a lot of coverage when it was first exposed, for example, the vulnerability that is the by far the biggest is often ignored – the end user.[1]

***"Most users have come to expect phishing attempts in their inbox. However, since SMS has not been associated, in the minds of typical end users, with this sort of attack, it is more likely to slip under most people's radars"***

The first problem is that 2FA doesn't actually verify the user's identity, only that he or she has access. This means that anyone with direct access to the device can pass through 2FA security measures as he can send himself the code. This would include any instance of a criminal with access to an unlocked device, but also potentially 'friendly fraud' from friends and family. People often feel much less guilty about digital theft than they would about physically stealing money. But this is not the biggest end user problem.

## The SMS phishing menace

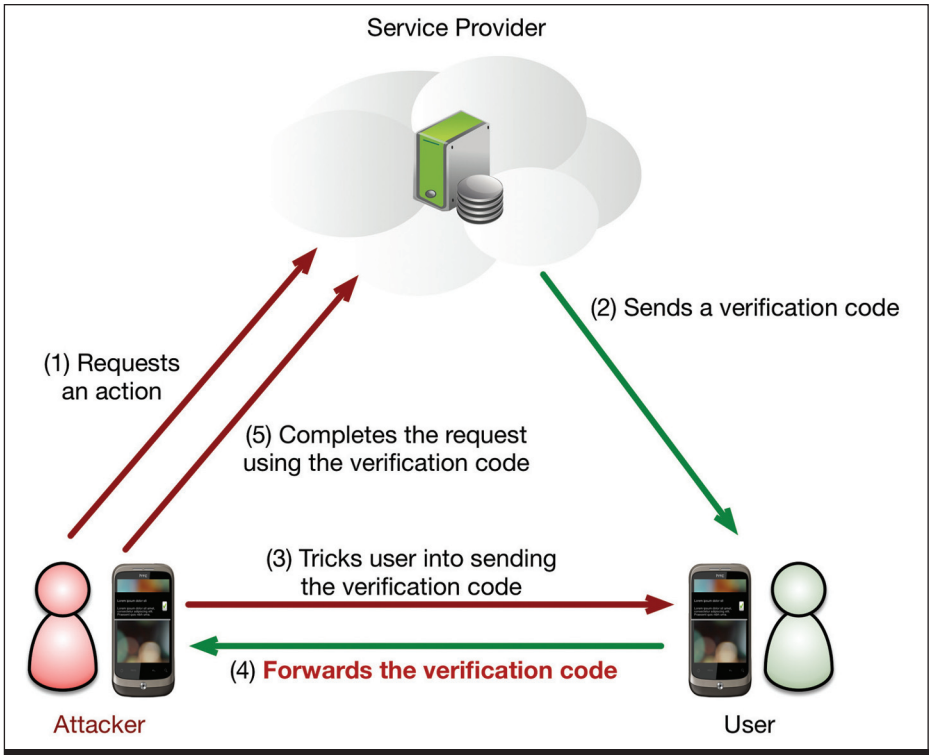
Thieves and fraudsters don't need to have the device in their hands, as 2FA is also vulnerable to remote phishing. We most often think of phishing attacks as taking place over email, targeting information such as passwords, but the same tactic can very easily be applied over SMS, targeting reset codes. One particularly powerful technique is the verification code forwarding attack (VCFA). For this approach, the criminals access a service provider and request an SMS code to reset the password for a particular user. Immediately afterwards, they send a fake text message to the same user, pretending to be the service provider and asking for the code 'as an additional verification measure'.

Over email this would ring a few alarm bells as most users have come to expect phishing attempts in their inbox. However, since SMS has not been associated, in the minds of typical end users, with this sort of attack, it is more likely to slip under most people's radars. The simplicity of a text message also means it's far easier to successfully fake than an email. There are no fonts or colours to match and less content means less chance to get something wrong for the criminal.

Likewise, very few people will care, or even notice, that the second (and fraudulent) text came from a different number, whereas a different email address can be a giveaway for more astute users. Most people are also aware that they won't normally be asked to send their passwords or reset codes via email, but there is no such habit when it comes to SMS. Unlike email, the fake messages are not routinely caught or filtered out, with no filters for users to plug in and little work from the carriers to police the issue.

## Effective attack

In a research experiment conducted at New York University, it was found that the VCFA technique can be incredibly effective – far more so than comparable email-based phishing attacks.[2] The study enlisted more than 300 volunteers, who were not aware that the experiment




**A verification code forwarding attack (VCFA) scenario. An attacker triggers the delivery of a verification code (for example, by using password reset feature) and tricks the user into forwarding the verification code. This is used to complete the password reset request and take over the user's account.**

involved SMS phishing: they were sent a variety of different messages designed after real SMS from their email provider. They then received simulated phishing messages, such as:

- "To continue using SMS-based verification for your account, please reply with the verification code we just sent to you."
- "Your account has been accessed from Nigeria. If you do NOT want to authorise further access, please reply with the confirmation code we just sent to you."

The most successful message was able to fool 50% of recipients into giving up their authentication code, which is an impossibly high result for most forms of social engineering. By comparison, most non-targeted email-based phishing attacks have a success rate of around 1%, with the very best reaching 2% or 3%.

This approach has taken a surprisingly long time to catch on – perhaps because it was previously so effective to conduct phishing campaigns over email. As email security has improved, however, criminals are exploring other avenues of attack. Whatever the reason, we have observed a definite upswing over the past couple of years.

However, as the experiment also shows, one can dramatically reduce the success rates of SMS phishing campaigns by redesigning the SMS message that gives the reset code to the end user. Somewhat simplified, these normally contain a code followed by a warning not to share the code in a risky manner: but by swapping the order of these two elements, the phishing success rate is reduced from 50% to 8%.

Hossein Siadati, an NYU PhD candidate involved in the research project, explained in the resulting paper: "We find that when a warning 'Please ignore this message if you did not request a code' precedes the authentication code, it stands up to social engineering attempts better than any other tested method."

While this is very encouraging, the number is still too high for comfort for many situations, calling for alternative 2FA approaches not involving SMS.

## No back-up to the back-up

Another major security flaw with 2FA is the lack of any kind of back-up in most cases – because *it* itself is supposed to be the back-up. The majority of 2FA systems are designed to support password-based login systems and protect them from phishing and fraud attempts, but there has been almost no regard for the potential for these tactics being used against the 2FA itself.

As email-based phishing has become so widespread, most service providers have implemented other ways to identify the user – for example by looking at their IP address and cookies. Even if someone is armed with the password, the site might initiate a 2FA request if something looks unusual. However, there are no similar measures in place when it comes to the 2FA code – whoever has the code is automatically assumed to be the correct user. If that code is compromised, whether through phishing or the device itself being accessed, the imposter can effectively assume the identity of the victim with no further barriers or alarm bells.

***"Whoever has the code is automatically assumed to be the correct user. If that code is compromised, whether through phishing or the device itself being accessed, the imposter can effectively assume the identity of the victim with no further barriers or alarm bells"***

Any service being breached in this way would mean severe repercussions for the victim, most obviously online payment, retail and anything else connected to financial data. The holy grail for any attacker is to gain access to an email account, a tactic known as email account compromise (EAC). While financial details can be exploited as a one-off opportunity before the bank takes

action, an email account can be used in much more subtle and insidious ways.

## The threat of EAC

Most immediately, the attacker can access anything in the inbox, which for a business account is likely to include a huge amount of confidential information such as intellectual property and corporate plans. This could either be sold on the black market or to a competitor, used for outsider trading, or simply leaked to cause enormous reputational and financial damage.

***"It is more important than ever for organisations to be aware that their workforce's digital identities may be compromised. Enterprises must be prepared for the threat of an employee's email being hijacked via 2FA"***

The infiltrator will also be free to comb through the victim's address book to find valuable contacts who can then be targeted with additional social engineering attacks – potentially launched from the corrupted account. Malicious emails sent from a legitimate account are by far one of the most dangerous and difficult to detect forms of cyber-attack, as very few security systems are designed to detect emails from real accounts. Criminals can also use the account to cover for any suspicious emails they send that may be intercepted – for example sending another message to say, "Hey, I just sent you an attachment but it may have been sent to spam, can you check?". As long as the messages themselves are well-written and don't contain obvious giveaways such as odd language choices, very few people will question such an email from a trusted contact.

EAC emails are far more difficult to detect than normal fraudulent messages, as they lack potential tells such as mismatched sender IDs. The good news is that they are not entirely unstoppable and it is possible to detect and prevent an EAC email by looking even deeper into different elements associated with the identity of the legitimate user. For example, an email security system could be set up to detect details about the user agent – the device used to send the email. For instance, a user might normally use a Mac with a 2560x1600 screen resolution, while the imposter who has hijacked their account might use a PC with an 1440x900 resolution.

This difference can be identified through the email itself, along with other signs such as the IP address. Taken together, these clues can point to a suspicious email even when the account address is genuine. The email can then be flagged for further examination to determine if there really is a malicious actor at work, or if the CEO happens to be using his or her spouse's PC for the afternoon.

## Can 2FA be saved?

The most obvious solution to the many security flaws in SMS 2FA is to abandon the text message as a verification measure – something we can expect to see happening with increasing frequency over the next year.

The clear successor is to move from a text-based numerical code to an authentication app such as Google Authenticator.[3] Whereas such codes can, of course, be requested by an attacker, it becomes harder for the criminal to succeed if the user is asked to volunteer something they *have* (the Authenticator code), instead of being asked to *give back what they have already been given* (the SMS-sent code). To further strengthen against attacks involving unauthorised users with access to the device, authenticator apps controlling access using biometrics would be a further step forward.

Although SMS 2FA is certainly on the way out, it will be some time before the change filters through all organisations thanks to its simplicity and popularity. While SMS remains so widespread and more attackers pick up on SMS phishing attacks, it is more important than ever for organisations to be aware that their workforce's digital identities may be compromised. Enterprises must be prepared for the threat of an employee's email being hijacked via 2FA and used to attack them from within.

### About the author

*Markus Jakobsson is an academic and an entrepreneur, as well as the author of a number of books and papers in information security. Using adversarial modelling from the field of cryptography, combined with related modelling of human behaviour, he analyses the security of real-life applications and designs improved security protocols. The efforts are often aimed at gaining a better understanding of and preventing phishing, pharming, malware spread, spam, spoofing and click fraud, but also address incentive problems, advertisement, and privacy. He is chief scientist at Agari, and has a PhD in computer science from UCSD.*

### References

1. Thomson, Iain. 'After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts'. The Register, 3 May 2017. Accessed May 2018. www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/.
2. Siadati, H; Nguyen, T; Gupta, P; Jakobsson, M; Memon, N. 'Mind your SMSes: Mitigating Social Engineering in Second Factor Authentication'. Computer & Security, Mar 2017, Vol.65, pp.14-28. Accessed May 2018. www.sciencedirect.com/science/article/pii/S016740481630116X.
3. 'Google Authenticator'. Wikipedia. Accessed May 2018. https://en.wikipedia.org/wiki/Google_Authenticator.