# Verification Code Forwarding Attack
## Short Paper

Hossein Siadati, Toan Nguyen, and Nasir Memon

New York University School of Engineering
{hossein,toan.v.nguyen,memon}@nyu.edu

**Abstract.** Major Internet service providers deploy *SMS-based verification* mechanisms to fortify the security of users' accounts for critical actions such as password reset and logging in from a new computer. In this paper, we describe a new type of phishing attack where an attacker triggers the delivery of a verification code from a service provider to a user and lures the user to forward the code to him so that he can bypass the SMS verification process. We call this a *Verification Code Forwarding Attack* (VCFA). The attacker can use VCFA to reset a password of a user's account or to get access to a 2-factor enabled account which he already knows its password (e.g., through leaked databases). We attribute the success of this attack to the lack of an effective and usable means for users to verify the service provider, the lack of context for the message sent, and an assumption about users' understanding of the authentication process. To show the susceptibility of the users to such an attack, we conducted an experiment with 20 mobile phone users and found that more than 25% of users were vulnerable against this type of attack. A semi-structured interview with the subjects of the experiment and a survey of 100 subjects on Amazon Mechanical Turk were done to explore possible causes for the success of this type of attack. We also discuss possible remediation.

## 1 Introduction

Guessable passwords [3], reusing passwords for different accounts [8, 5], breaches of password databases [12, 2], an abundance of malware and the ease of which the devices get infected by trojans and key-loggers easily give attackers access to passwords. As a result, for critical actions such as password recovery and high risk authentication (e.g., log in from a new device) an auxiliary factor is needed to make the system more secure. One prevalent approach adopted by service providers leverages a resource assumed to be in control of the user, such as a phone number or an email address. In one such example of the scheme, advertised as a 2-step or 2-factor verification, the service provider sends a *nonce* in the form of a *verification code* to the user. The user presents this verification code back to the service provider via a channel requested by the service provider. Since the user who is being authenticated is assumed to be in control of this resource, the address of the resource is likely to be unknown to an attacker, and the nonce is random, the requested authentication is then completed. The rationale is that to circumvent such a mechanism, an attacker has to be in *control* of this auxiliary channel or resource. In this work, we show that authentication schemes that utilize such an auxiliary resource can be potentially circumvented without gaining control of the channel but by other means such as social engineering.

For example, we show that a commonly used authentication scheme where a verification code is sent to the user's mobile phone by an SMS message can potentially be compromised by luring the user to send the code to the attacker. We call this a Verification Code Forwarding Attack (VCFA).

In a VCFA attack, the attacker triggers the delivery of a verification code to a victim and shortly after that, the attacker sends a direct SMS to the victim and phishes him or her to forward the code. If the victim forwards the code, the attacker can successfully bypass the SMS verification and get access to the victim's account.

Attackers can use VCFA in three attack scenarios. The first scenario is *password reset*. In this attack, the attacker initiates a password recovery request on a service provider website by entering victim's username or email address and chooses to receive a verification code via SMS message. Shortly after the verification code is sent to the victim, the attacker will phish the victim to steal the verification code and complete the password reset. The attacker needs to know the phone number of the victim in order to phish him or her. For this, the attacker can easily search the public records, social networking websites, data from leaked databases of information or employ social engineering techniques. In a second scenario, the attacker knows the username and password of a victim (perhaps through leaked databases or other hacking techniques), logs into the victim's account from a new machine and then lures the victim to forward the verification code. The access to the victim's account as a result of this attack is at least for one session, but also can be permanent depending on the victim's account settings. The last scenario belongs to *spam account creation* where a fraudster or spammer creates a verified account without giving out any traceable information. In this attack, the spammer enters a random phone number as his verification number at the time of account creation. Then he follows the described steps to phish the verification code.

In this paper, we study this new type of phishing attack and the root causes of why it is successful. In particular, these are our contributions in this research:

- Using a small scale experiment on 20 subjects, we show that more than 25% of users are susceptible to VCFA.
- By conducting a semi-structured interview, we systematically study the reasons why people fall or do not fall for this attack.
- Using a survey on about 100 Amazon Mechanical Turk workers that have enabled SMS-based verification for their Gmail accounts, we validate our findings on a larger and more diverse pool of subjects.

**Paper organization**: After briefly introducing background in Section 2, we detail our study procedures and findings in Section 3. We discuss the root causes of the problem and possible remediations in Section 4.

## 2 SMS-based verification and its security

SMS-based verification is a subset of *two-factor authentication* (2FA) mechanisms where a one-time password is used as a second factor for authentication. SMS-based verification is not able to provide security against a phishing attack [14]. The argument is that in a successful phishing attack, the attacker will

lure a victim to enter the one-time password as well. This attack is deployed by attackers in the wild [4]. SMS-based verification also does not provide protection against the existence of malware on mobile devices or workstations [14, 7] because by using the malware, the attacker can capture the one-time passwords as well as hijacking a session after the authentication process is done. The malware attack on SMS-based verification has been in use by attackers [13, 1]. The SMS-based verification, however, provides protection against *known-password-attack* when the user-chose password is known by the attacker, for example based on a leaked database of passwords. For an account protected by SMS-based verification, an attacker who knows the password still can not log in to the account because he does not have access to the verification code. However, such an attacker can launch a VCFA attack to get the user to forward the verification codes, as discussed in this paper.

Several research work have previously studied social engineering techniques and phishing attacks [9–11, 15]. Dhamija et al. [6] have studied the reasons why phishing is successful. Major reasons are visual techniques that the attackers use to deceive users into believing that the URL and the webpage are authentic.

Although there are similarities between the known email-based phishing attacks, Smishing (SMS-based phishing where a phishing link is sent via SMS), and VCFA, there are several differences concerning the reasons for their success and needed countermeasures against them. Firstly, in a VCFA attack, no URL is included in the phishing messages and victims do not need to visit a phishing website. Secondly, a successful VCFA attack needs a victim to forward only a verification code, mostly, a random sequence of digits. In comparison, a victim of traditional phishing attack has to enter widely known sensitive credentials such as password, credit card numbers, or SSN numbers into a website. Thirdly, there are a few indicators such as the sender's email address or the URL of the phishing website that can be used to verify the authenticity of a phishing message and website. In a VCFA attack, however, the victim only has the phone number of the sender and it is much harder to verify the sender of a message based on that alone. These differentiating elements suggest the study of reasons for success of VCFA attack and its remediation.

## 3 Study Procedures

We conducted this research in three phases. The first phase was a small scale phishing experiment on 20 subjects. Next, we interviewed the subjects. Finally, we extracted a handful of hypotheses from the interviews and evaluated them in a larger scale by surveying 100 subjects on Amazon MTurk.

### 3.1 Experiment

For the sake of the experiment, we imitated a VCFA attack using messages similar to Google's messages. We bought two 10-digit U.S.A phone numbers, one for imitating the role of a service provider (e.g., Google in our experiment) and the other one for imitating the role of the attacker (e.g., sending phishing message to subjects). The area code for the phone numbers were Mountain View, CA (the area code for Google's headquarters) to make the first message appear more legitimate and the second one more deceptive. We randomly selected 20 subjects

from the contact list of the experimenters. The subjects included 10 males and 10 females, mostly aged between 25-35. 70% of the subjects were students. We were granted an IRB exemption from our institution for this research. We sent two messages to each subject from two different numbers. The first message was: ***"Your Google verification code is [6-digit code]."*** The style of the message exactly followed the Google's message for verification code. It did not include username or any user identifying information. It also did not include the reason why the user is receiving this message. 30 seconds later, we sent the second message: ***"Please verify that your phone is still associated with your Gmail account by replying to this message with the code we have just sent to you."***

**Experimental results.** 5 out of 20 subjects forwarded the verification codes. This is translated to 25% success for the VCFA attack.

### 3.2 Semi-structured interview

We interviewed 10 out of 20 subjects of our experiments, 5 of those who fell for phishing and 5 who did not.

**Findings.** After completing the interviews, we documented the responses and analyzed them to find themes and significant experiences. Because of the space constrains, we only report some of the findings and refer the readers to the long version of this paper.

Subjects listed different reasons for enabling the SMS-based 2FA for their Gmail accounts. The major reason was improving security of their accounts. One subject mentioned that she has enabled the 2FA because of the need for logging into her account from insecure machines at the university's library and laboratories. Since the verification codes are sent to her phone, she thought it was safe to enter her password on potentially insecure computers.

70% of subjects that we interviewed mentioned that they did not pay attention to the phone number that they received the *Message I* from. Indeed, they believed that the message was sent by Google. Apart from two subjects who did not fall for VCFA, other subjects did not notice that the phone number that was used for *Message II* was different from the first phone number. Another interesting finding was that the subjects have seen Google using different phone numbers with different lengths (i.e., short codes vs. 10-digit numbers) for sending verification codes. They did not have a clear understanding of what a Google phone number looks like. These observations explain the core problems of SMS-based verification since SMS system does not provide any effective and usable means for users to verify the sender of messages.

In general, users found the second message (message sent by the attacker) convincing because Google's message does not include any context or reason why the user has received a verification code. Therefore, the second message can alter users' perception and convince them to forward the code. This lack of context is another problem in design of the verification messages in most of the SMS-based verification systems.

### 3.3 Survey

Following the interviews, we formed a survey in order to measure the extent and prevalence of the insights we gained from the interviews. Our questionnaire was

composed of questions about demographics (i.e., age and gender), and users' usage of SMS-based verification (i.e., frequency of usage of SMS-based verification including "every log in", "log in from a new computer", and "password recovery"). We also asked about the reasons for using SMS-based verification (i.e., "log in from insecure computers" and "account being hacked before.") We asked if they check the phone number of the sender of a verification message. In addition, we asked two different questions to discover the perceptions of users about a VCFA attack in different stages of the attack. Firstly, we asked users if they have ever received an unwanted verification code and what their perception would be if they received one. Then, we asked them to consider a hypothetical scenario in which Google asks them to forward a verification code. Using these questions, we measured the success rate of the VCFA attack on a larger scale. We ran the survey on Amazon MTurk. We asked MTurkers to take survey only if they have enabled SMS-based 2-step verification for their Gmail account. A cleaning process to exclude the unqualified subjects resulted in 98 reliable responses.

**Results.** 66% of participants in our survey were male, and 90% of participants were between 18 and 35 years old. 8% of participants use SMS-based verification every time they log into Gmail. 66% use it for logging in from a new computer, and about 22% for password reset. We asked users why they chose to use the SMS-based verification. 62% mentioned that they enabled it because they log in from insecure computers, and 22% have enabled it because their accounts have been hacked before.

We asked the participants if they check sender's phone number of verification messages. 38% of participants reported that they check the phone number to make sure it comes from Google. However, 30% of participants did not have any idea about the length of the phone number that Google uses to send the verification codes (i.e., short code vs 10-digit number). 58% of participants believed that they received the verification code from the same number whereas others thought Google uses different numbers to send verification codes. This demonstrates that current settings for SMS-based verification does not offer any effective and usable mechanism for users to verify the sender of the messages.

We asked participants how they would feel if they received an unwanted verification code. 67% of participants believed that it would mean that somebody is hacking their account, 11% believed this is the result of a flaw in the Google's system, 22% of participants did not know why this may happen. We can see that a considerable number of users are not aware of the possibility of a misuse or an attack based on verification codes.

We asked participants what they would do if Google asks them to forward a verification code via SMS. 20% of participants answered that they would forward the verification code, meaning that they would fall for this attack given the fact that Google never asks users to do so. It is important to notice that we notified the participants about the possibility of an attack by adding a choice to answers as follows: "I think somebody is hacking me". Therefore, the expected yield of this attack might be more than 20% in reality.

## 4 Conclusion

A noticeable number of the users are susceptible to VCFA attack. We attribute the success of this attack to the lack of an effective and usable means for users to verify the service provider and the lack of context for the message sent. Another reason is the assumption about users' understanding of how this authentication process works and their awareness of the possibility of a misuse based on verification codes. A potential quick fix by service providers would be to use a list of publicly announced phone numbers that users should expect to get their messages from. Possible long-term remediation would be to augment a naming system to SMS system so users can see the name of a service provider who sends a message. Another simple fix is to add context to verification code messages indicating why the user received a verification code. Another fix includes appending a warning text such as "DO NOT FORWARD THE VERIFICATION CODE" to remind the importance of the code. The number of subjects in our experiment and the process of recruiting the subjects in this experiment only suit a pilot study. We are conducting a larger scale study to verify our results and to measure the success of suggested list of potential remediation.

## References

1. Bankinfosecurity. Malware bypasses 2-factor authentication. http://www.bankinfosecurity.com/malware-bypasses-2-factor-authentication-a-7090/op-1. Accessed: 2015-08-25.
2. J. Bonneau. The gawker hack: how a million passwords were lost. https://www.lightbluetouchpaper.org/2010/12/15/the-gawker-hack-how-a-million-passwords-were-lost/. Accessed: 2015-08-25.
3. J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *SP*, pages 538–552. IEEE, 2012.
4. Citizenlab. London calling: Two-factor authentication phishing from Iran. https://citizenlab.org/2015/08/iran_two_factor_phishing/. Accessed: 2015-08-25.
5. A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *NDSS*, 2014.
6. R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *CHI*, pages 581–590. ACM, 2006.
7. A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi. On the (in) security of mobile two-factor authentication. In *Financial Cryptography and Data Security*, pages 365–383. Springer, 2014.
8. B. Ives, K. R. Walsh, and H. Schneider. The domino effect of password reuse. *Communications of the ACM*, 47(4):75–78, 2004.
9. T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Communications of the ACM*, 50(10):94–100, 2007.
10. M. Jakobsson and S. Myers. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft.* John Wiley & Sons, 2006.
11. M. Jakobsson, A. Tsow, A. Shah, E. Blevis, and Y.-K. Lim. What instills trust? a qualitative study of phishing. In *Financial Cryptography*, pages 356–361. Springer, 2007.
12. J. Kirk. Dating site eHarmony confirms password breach. http://www.computerworld.com/article/2504089/security0/dating-site-eharmony-confirms-password-breach.html. Accessed: 2015-08-25.
13. N. Perlroth. Hackers find way to outwit tough security at banking sites. http://bits.blogs.nytimes.com/2014/07/22/hackers-find-way-to-outwit-tough-security-at-banking-sites. Accessed: 2015-07-20.
14. B. Schneier. Two-factor authentication: too little, too late. *Commun. ACM*, 48(4):136, 2005.
15. M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 601–610. ACM, 2006.