H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-07

WHAT IS SMSHING AND HOW TO DEFEND AGAINST IT

1. Background:

Smishing is a phishing cybersecurity attack carried out over mobile text messaging, also known as SMS phishing.

As a variant of phishing, victims are deceived into giving sensitive information to a disguised attacker. SMS phishing can be assisted by malware or fraud websites. It occurs on many mobile text messaging platforms, including non-SMS channels like data-based mobile messaging apps.

2. Definition of SMShing

As the definition of smishing suggests, the term combines "SMS" (short message services, better known as texting) and "phishing." To further define smishing, it is categorized as a type of social engineering attack that relies on exploiting human trust rather than technical exploits.

When cybercriminals "phish," they send fraudulent emails that seek to trick the recipient into clicking on a malicious link. Smishing simply uses text messages instead of email.

In essence, these cybercriminals are out to steal your personal data, which they can then use to commit fraud or other cybercrimes. Typically, this includes stealing money — usually yours, but sometimes also your company's money.

Cybercriminals often use one of two methods to steal this data:

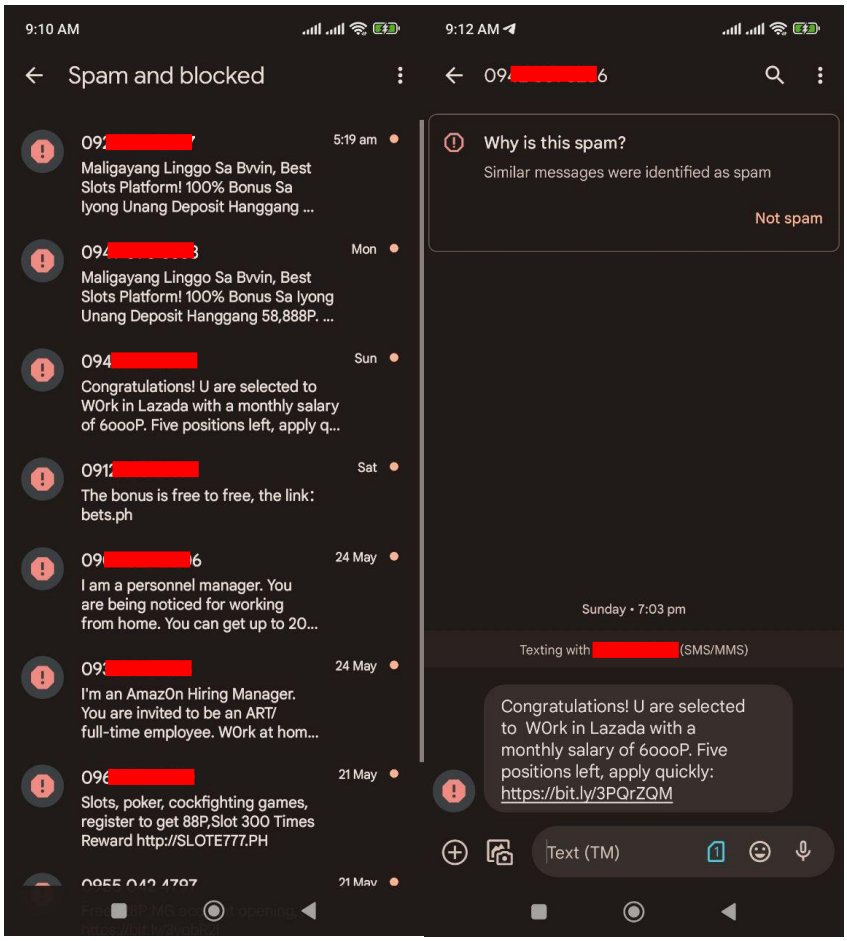
a. Malware: The smishing URL link might trick you into downloading malware — malicious software — that installs itself on your phone. This SMS malware might masquerade as a legitimate app, tricking you into typing in confidential information and sending this data to the cybercriminals.

b. Malicious Website: The link in the smishing message might lead to a fake site that requests you to type sensitive personal information. Cybercriminals use custom-made malicious sites designed to mimic reputable ones, making it easier to steal your information.

Smishing text messages are often purporting to be from your bank, asking you for personal or financial information such as your account or ATM number. Providing the information is equivalent to handing thieves the keys to your bank balance.

As more and more people use their personal smartphones for work (a trend called BYOD, or "bring your own device") smishing is becoming a business threat as well as a consumer threat. So, it should come as no surprise that smishing has become the leading form of malicious text messages.

Cybercrime aimed at mobile devices is rising, just as mobile device usage is. Aside from texting being the most common use of smartphones, a few other factors make this a particularly insidious security threat. To explain, let's unpack how smishing attacks work.



3. How SMShing work?

Deception and fraud are the core components of any SMS phishing attack. As the attacker assumes an identity that you might trust, you are more likely to succumb to their requests.

Social engineering principles allow smishing attackers to manipulate a victim's decision-making. The driving factors of this deception are three-fold:

a. Trust:

By posing as legitimate individuals and organizations, cybercriminals lower their target's skepticism. SMS texts, as a more personal communication channel, also naturally lower a person's defenses against threats.

b. Context:

Using a situation that could be relevant to targets allows an attacker to build an effective disguise. The message feels personalized, which helps it override any suspicion that it might be spam.

c. Emotion:

By heightening a target's emotions, attackers can override their target's critical thinking and spur them into rapid action.

Using these methods, attackers write messages that will get a recipient to take action.

Typically, attackers want the recipient to open a URL link within the text message, where they then are led to a phishing tool prompting them to disclose their private information. This phishing tool often comes in the form of a website or app that also poses under a false identity.

Targets are selected in many ways but usually are based on their affiliation to an organization or a regional location. Employees or customers of a specific institution, mobile network subscribers, university students, and even residents of a given area can be targets.

An attacker's disguise is usually related to the institution they wish to gain access to. However, it can just as easily be any mask that will help them acquire your identity or financial information.

Using a method known as spoofing, an attacker can hide their true phone number behind a decoy. Smishing attackers may also use "burner phones" — cheap, disposable prepaid phones — to further mask the origin of the attack. Attackers are known to use email-to-text services as another means of hiding their numbers.

Step-by-step, an attacker, will carry out their attack in a few key phases:

a. Distribution of the text message "bait" to targets.

b. Compromising the victim's information via deception.

c. Execution of the desired theft using the victims' compromised information.

An attacker's smishing scheme is successful once they've used your private information to commit the theft they aimed for. This goal could include but is not limited to directly stealing from a bank account, committing identity fraud to illegally open credit cards, or leaking private corporate data.

4. SMShing Examples

a. COVID-19 SMShing

COVID-19 smishing scams are based on legitimate aid programs designed by government, healthcare, and financial organizations for recovery from the COVID-19 pandemic.

Attackers have used these schemes to manipulate victims' health and finance fears for committing fraud. Warning signs can include:

- Contact tracing that asks for sensitive info (social security number, credit card number, etc.)
- Financial Reliefs.
- Public health safety updates.

b. Financial Services SMShing

Financial services smishing attacks are masked as notifications from financial institutions. Nearly everyone uses banking and credit card services, making them susceptible to both generic and institution-specific messages. Loans and investing are also common premises in this category.

An attacker poses as a bank or other financial institution for an ideal disguise to commit financial fraud. Features of a financial services smishing scam may include an urgent request to unlock your account, being asked to verify suspicious account activity, and more.

c. Gift SMShing

Gift smishing suggests the promise of free services or products, often from a reputable retailer or other company. These can be giveaway contests, shopping rewards, or any number of other free offers. When an attacker elevates your excitement by proposing the idea of "free," this serves as a logic override to get you to take action faster. Signs of this attack can include limited time offers or exclusive selection for a free gift card.

d. Invoice or Order Confirmation SMShing

Confirmation smishing involves a false confirmation of a recent purchase or billing invoice for a service. A link may be provided for a follow-up to manipulate your curiosity or prompt immediate action to trigger fear of unwanted charges. Evidence of this scam may involve strings of order confirmation texts or the absence of a business name.

e. Customer Support SMShing

Customer support smishing attackers pose as a trusted company's support representative to help you resolve an issue. High-use tech and e-commerce companies like Apple, Google, and Amazon are effective disguises for attackers in this premise.

Typically, an attacker will claim there is an error with your account and give you steps to resolve it. The request can be as simple as using a fraudulent login page, while more complex schemes may ask you to provide a real account recovery code in an attempt to reset your password. Warnings of a support-based smishing scheme include an issue with billing, account access, unusual activity, or resolving your recent customer complaint.

5. Recommendations

a. How to Prevent SMShing

The good news is that the potential ramifications of these attacks are easy to protect against. You can keep yourself safe by doing nothing at all. In essence, the attacks can only do damage if you take the bait.

That said, be mindful that text messaging is a legitimate means for many retailers and institutions to reach you. Not all messages should be ignored, but you should act safely regardless.

There are a few things to keep in mind that will help you protect yourself against these attacks.

- Do not respond. Even prompts to reply like texting "STOP" to unsubscribe can be a trick to identify active phone numbers. Attackers depend on your curiosity or anxiety over the situation at hand, but you can refuse to engage.

- Slow down if a message is urgent. You should approach urgent account updates and limited time offers as caution signs of possible smishing. Remain skeptical and proceed carefully.

- Call your bank or merchant directly if doubtful. Legitimate institutions don't request account updates or login info via text. Furthermore, any urgent notices can be verified directly on your online accounts or via an official phone helpline.

- Avoid using any links or contact info in the message. Avoid using links or contact info in messages that make you uncomfortable. Go directly to official contact channels when you can.

- Check the phone number. Odd-looking phone numbers, such as 4-digit ones, can be evidence of email-to-text services. This is one of many tactics a scammer can use to mask their true phone number.

- Opt to never keep credit card numbers on your phone. The best way to keep financial information from being stolen from a digital wallet is to never put it there.

- Use multi-factor authentication (MFA). An exposed password may still be useless to a smishing attacker if the account being breached requires a second "key" for verification. MFA's most common variant is two-factor authentication (2FA), which often uses a text message verification code. Stronger variants include using a dedicated app for verification (like Google Authenticator) are available.

- Never provide a password or account recovery code via text. Both passwords and text message two-factor authentication (2FA) recovery codes can compromise your account in the wrong hands. Never give this information to anyone, and only use it on official sites.

- Download an anti-malware app. Products like Kaspersky Internet Security for Android can protect against malicious apps, as well as SMS phishing links themselves.

- Report all SMS phishing attempts to designated authorities.

Remember that, like email phishing, smishing is a crime of trickery — it depends on fooling the victim into cooperating by clicking a link or providing information. The simplest protection against these attacks is to do nothing at all. If you don't respond, a malicious text cannot do anything.

b. What to do if you become a victim of SMShing

Smishing attacks are cunning and may have already victimized you, so you'll need to have a recovery plan in place.

Take these important actions to limit the damage of a successful smishing attempt:

- Report the suspected attack to any institutions that could assist.
- Freeze your credit to prevent any future or ongoing identity fraud.

- Change all passwords and account PINs where possible.
- Monitor finances, credit, and various online accounts for strange login locations and other activities.

Each of these steps has a substantial weight for your protection after a smishing attack. However, reporting an attack not only helps you recover, but keeps others from falling victim as well.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it*