The Beginner’s Guide to Phishing

I’m White Ops’ resident phisher. As an InfoSecurity team member, it’s my job to make sure everything we do is secure and free from cybercriminals so we can fight for you. To do this, I deploy fake phishing attempts on White Ops’ own Humans, not to shame them when they click on a link (though they sometimes out themselves out of frustration), but to show just how realistic—*human*, even—a phishing attempt can appear. While we must stay particularly vigilant given our line of work, phishing can target anyone. Phishing is a low-risk, high-reward social engineering attack that uses electronic communication to exploit an end user into providing personal information or clicking on malicious links.

Without the proper literacy around how to spot phishing attempts, you can open yourself to all sorts of malware and fraudulent behavior. Especially since phishing has come a *long* way from the infamous foreign prince scams. Cybercriminals have evolved their tactics making it even harder to catch a phish.

Are there different types of phishing?

Phishing isn’t just one type of attack, it’s a category of attacks. There’s spear phishing, smishing, vishing, and whaling attacks:

Spear Phishing is a *targeted* phish usually aimed at a specific user or organization. In order to do this, fraudsters use personal information that is discoverable online to contact you. This information can be found on areas of the internet that are freely available, such as on social media. These typically take the form of emails, such as Figure 1. You can see that the email is vague and urgent to entice someone to click.

IT Department
to me

ATTENTION

Your computer has recently connected to our network without using our company VPN. Another security infraction will result in your account being suspended.

Please view our instructions on how to use our VPN here.

Download VPN here.

Figure 1: Example of a spear phishing email

Smishing is a SMS phish that usually asks you to do something, such as provide some sort of personal information or click on a link. This phish is particularly deceptive because people are more likely to trust a text message vs an email. In Figure 2, you can see how innocuous of a text they can be. Usually a smishing attack will have a very broad request to have you download a malicious app or go to a fake website where you have to enter PII (personal identifiable information) data.

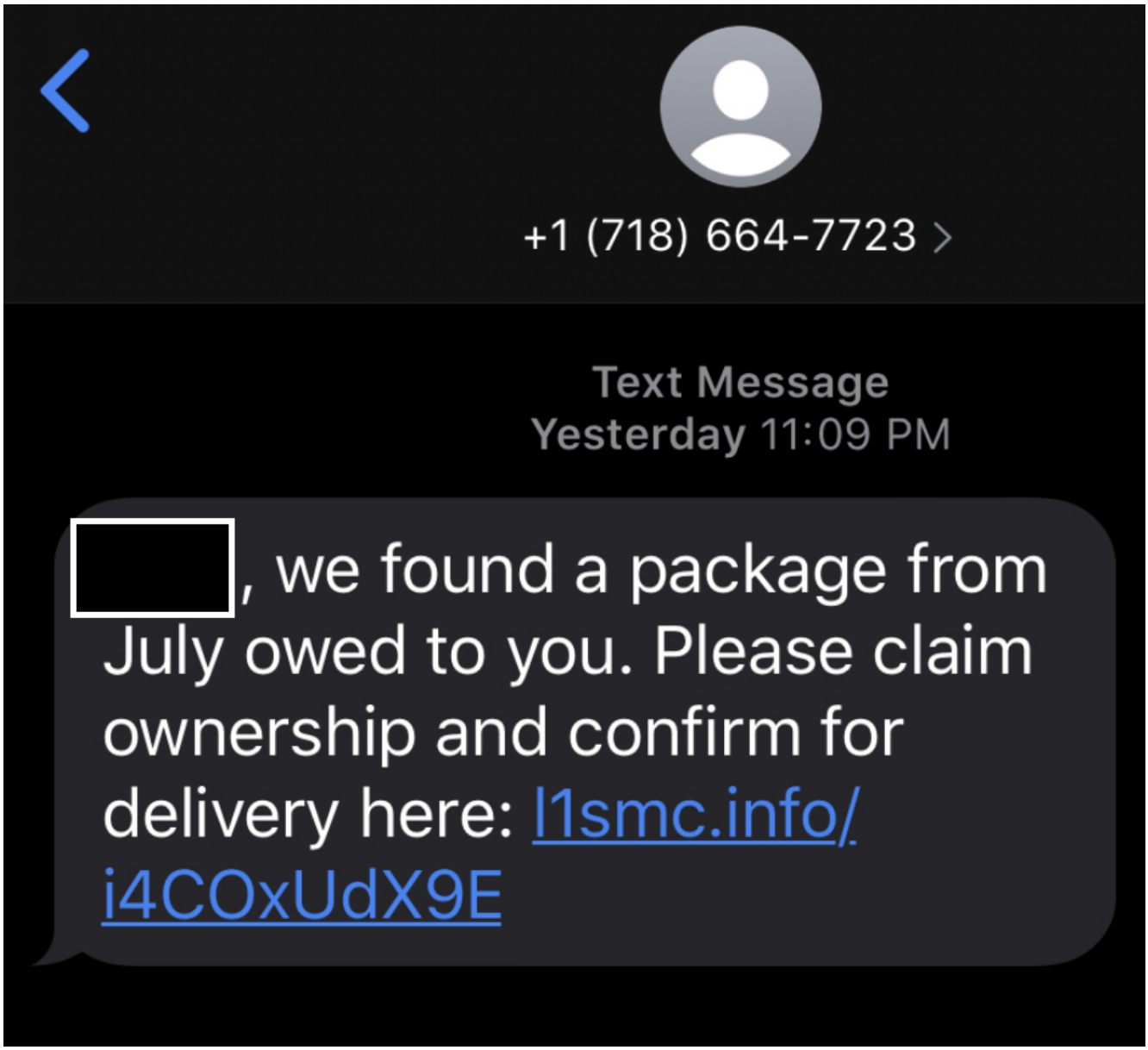

Figure 2: An example of smishing

Vishing is a phish that takes place over the phone where the fraudsters are asking you to provide some sort of personal information. The surge of VOIP technology has made it easier for adversaries to spoof

caller IDs. We see this attack happen a lot where fraudsters pretend to be the IRS saying you owe them money or you'll go to jail. They do this to get social security numbers or any of your PII data.

Whaling is a type of spear phishing attack that is more focused on high profile targets. With other types of phishing, the target is a group of people - it's not about each individual. Whaling doubles down on specific people and targets them. It's called whaling because they're going after bigger targets like high-level executives. Typically, the fraudsters will pretend they're a higher-level executive to get people to divulge sensitive company information. For instance, they will target a VP by pretending to be the CEO. Figure 3 shows a whaling attempt directed at a White Ops employee. The phish uses urgency in both the language and by having it appear to be from White Ops CEO & Co-founder, Tamer Hassan. Additional hallmarks include the wonky grammar, stray letters, and incorrect capitalization of "iPhone." This is a pretty obvious phish to us since Tamer wouldn't ask people to run "errands" for him.

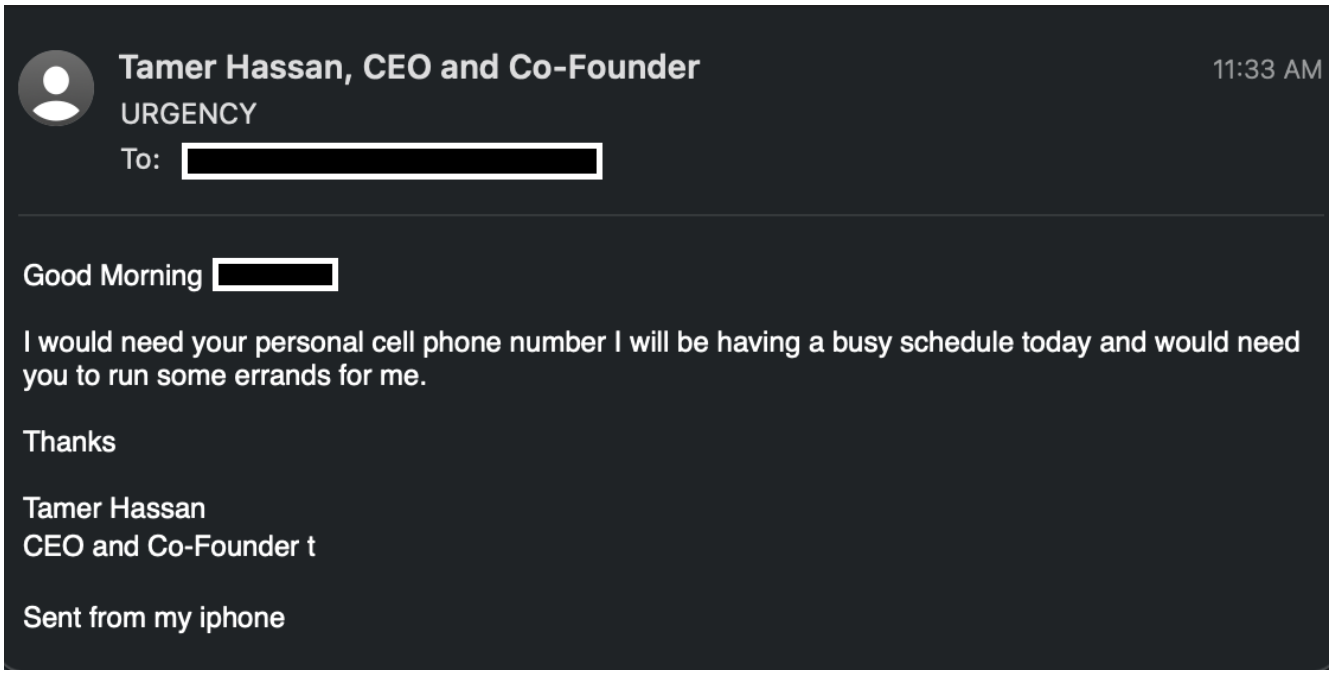

Figure 3: Example whaling attempt a White Ops employee received.

What should I look out for?

Thankfully, once you learn the hallmarks of phishing attempts they become easier to spot and report. There are several elements you should check before clicking on any links:

- **Suspicious email addresses**: If you were receiving an email from Linkedin you would expect it to come from a linkedin.com domain not linkedin@gmail.com. Always check the "reply to" email to find spoofed senders.
- **Suspicious links in the email/SMS:** You can determine the legitimacy of the link by hovering over it before clicking. When analyzing the URL, check to make sure it starts with an https:// not http://. You can also check the site's certificate to see who it's issued to. A fraudulent link usually looks like XYZ
- **Grammatical errors**: Always check for grammatical errors, not just spelling mistakes.
- **Unnecessarily urgent**: Phishers love to ask you to do something *right now or else.* Whether that is clicking on a link or replying to an email, they want you to act ASAP. They do this to try to scare or threaten you, such as closing down an account or confirming activity.

- **Generic greetings**: The email may start with Dear Sir or Madam or Dear User, which isn't how people normally talk to each other when writing emails. It usually isn't personalized unless it's spear phishing.
- **Offers that are too good to be true**: That's because they are! Don't respond or click on any links in these emails.

How can I protect myself?

It is possible to be proactive in protecting your information from phishing attacks.

- **Keep an eye on the news**: New forms of phishing are evolving each day and major attacks will usually be covered. If you know what to look out for it can be easier to spot these types of attacks. If you're not sure if something is a phish, copy a piece of text from the body of the email and paste it into a search to see if it's a known phishing email.
- **Update your operating system regularly**: Attackers try to leverage known vulnerabilities in systems so it's in your best interest to stay up-to-date on the latest security updates on all your devices. The best solution is to enable automatic updates on all your devices to ensure you're on the latest and greatest OS. Also, make sure your browser of choice automatically updates as well.
- **Don't open attachments or links:** This is especially important when receiving an email from an unknown sender. If you don't know the sender, don't open the attachment. Examples can include PDF's. Excel, Word, or Powerpoint attachments. Also, be sure to hover over the link and determine the legitimacy of the link before clicking.
- **Enable firewalls**: Turn on the firewall on your device and network to ensure you filter out outside attackers.
- **Avoid answering unknown calls:** It's good practice to not answer a call from an unknown caller ID. Never give personal information over the phone as well, especially if they sound unrealistically urgent.
- **Regularly backup your devices:** In the event your device is compromised, it's good practice to restore from a known good backup.
- **Contact the real sender:** If you received a suspicious email from a close friend, relative, or business, reach out to them to see if the message was intended to be sent. You may be doing them a favor by showing how they might be potentially compromised.

I fell for a phish, what do I do now?

Don't panic! If you believe your credentials have been compromised, alert your leadership or security team as soon as possible, then go to the sites you use these credentials on and change them. Additionally, enable 2FA (Two Factor Authentication) if you haven't already. Use a password manager and ensure you have unique passwords on every site you use, and enable 2FA on any site that offers it You should also check *all* your online accounts to see if there is any unusual activity associated with them.

If these credentials are used for a financial institution, I would contact them immediately and explain the situation. Consider freezing your credit if you're concerned that the attack may have resulted in access to your social security information. Use it as a learning opportunity and teach family and friends what to look out for so they don't fall for the same attack. If you click on a link and you believe your device is infected with malware, restore from a known good backup or factory restore the device.

Even when someone does their best to be safe online, they can still get caught in a phish net (pun intended). As long as you follow these steps, you'll be better off the next time a fraudster tries to mess

with you.