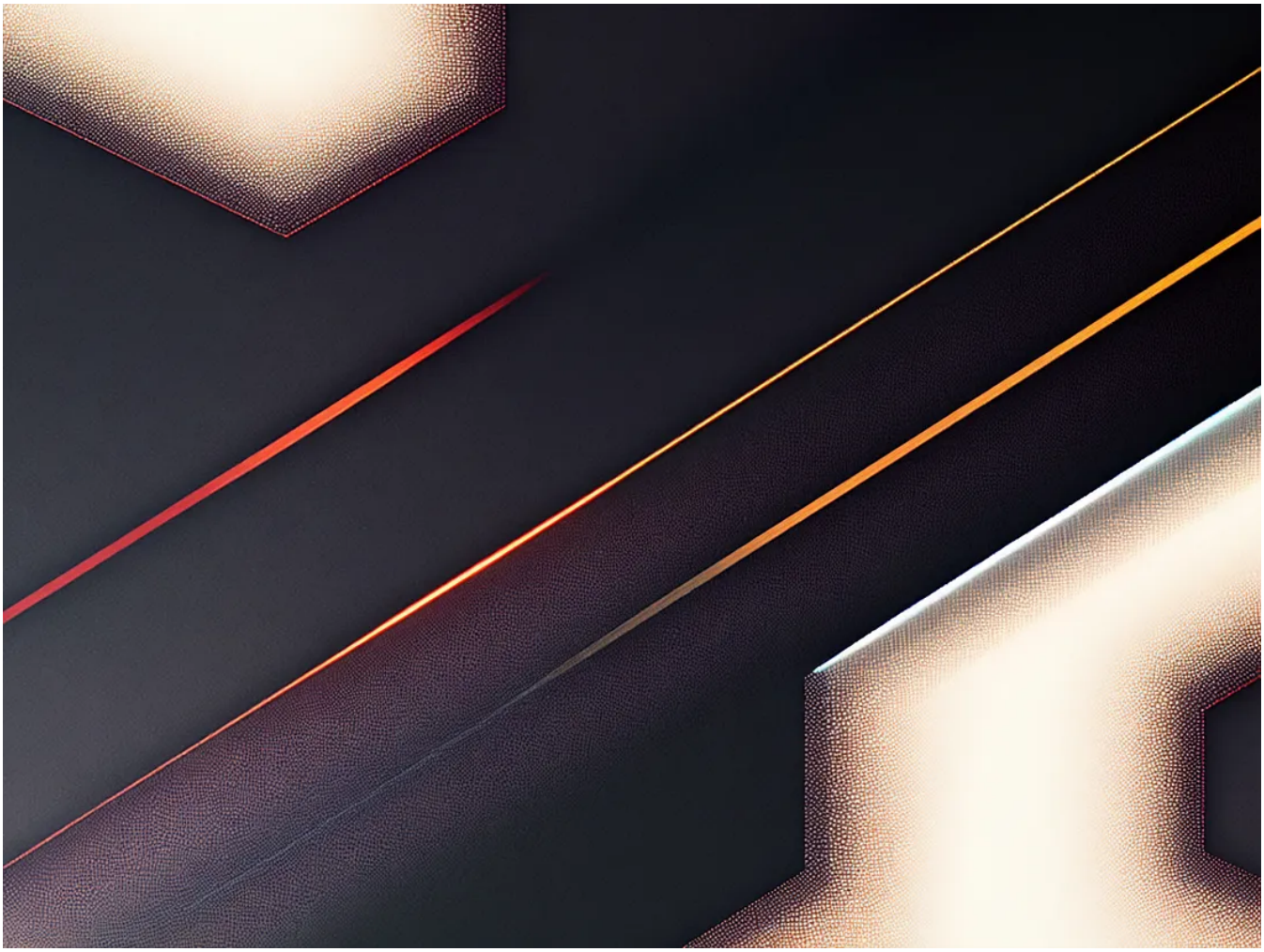
Phishing vs Smishing vs Vishing

Daniel Iwugo
Published in InfoSec Write-ups
4 min read · Jun 24



Abstraction v1 ¦ Credit: Mercury

You've probably heard of Phishing. It's a social engineering attack where an attacker tries to get you to open an email, click a link or carry out a conversation through your email. But what about Smishing and Vishing?

In this mini article, we will take a look at Phishing, Smishing and Vishing, infamous hacks that involved such techniques and some basic mitigations that both individuals and organisations can use to counter such tactics.

Without further a due, lets jump in.

Phishing

Phishing is the most widely recognized and prevalent attack of the three. It usually happens via email but can also occur through alternative communication platforms like instant messaging or social media 📨. Phishing emails frequently mimic legitimate sources such as banks, online services, or government agencies.

By generating a sense of urgency or exploiting curiosity, an attacker deceives recipients into clicking on harmful links or downloading malicious attachments. These deceptive tactics can result in the exposure of sensitive information or the installation of malware on the victim's device.

Ukranian Cybercriminal Gang

On March 30, 2023, the Cyberpolice of Ukraine working with law enforcement from Czechia arrested members of a cybercriminal gang that set up phishing sites to target Europeans.

The group had set up over a hundred phishing websites that sold products on the market at high discounts. However, the sites were fake and the gang used the financial information from users to take their money from their accounts. The group are estimated to have victimised 1000 people and earned $4.22 million as profits.

The Hacker News added that charges have been laid against the group, with a maximum sentence of up to 12 years in prison if convicted 💀.

Smishing

Smishing distinguishes itself by the use of SMS (Short Message Service) or text messages on mobile devices 📱 . Crafty attackers employ this method by dispatching text messages masquerading as trustworthy sources, often mimicking reputable banks or service providers. Using strategies similar to phishing, smishing aims to manipulate unsuspecting recipients by creating a sense of urgency or presenting seemingly irresistible offers that are too good to be true.

These text messages commonly contain embedded links that once clicked, redirect users to malicious websites or entice them to divulge sensitive information through a text reply. The success of smishing attacks hinges on capitalizing on the immediacy and nature of text messaging, which in turn tricks individuals.

The Trinitarians financial bust

On May 9, 2023, the National Police of Spain arrested 40 people in relation to a phishing and smishing campaign. In order to carry out the campaign, the group created a phishing website that looked like a legitimate bank portal victims were used to. Next, a smishing text was sent to multiple bank customers, alerting them to solve a security problem using the link to the phishing page.

The unsuspecting customer would login into the fake website with real credentials, giving the attackers what they need. The attackers would then use the compromised credentials on the real website to apply for loans and linked the bank cards of victims to virtual wallets.

The money went through various other systems to minimise tracking and was used to purchase drugs, pay lawyers and pay for the gang's other activities. The group allegedly scammed over 300,000 people and made at least $760,000 before getting busted.

Vishing

Vishing, which is short for "voice phishing," refers to a deceptive technique where attackers use phone calls or voice communication to trick people 📞. They often pretend to be representatives from trusted entities like banks or tech support, aiming to obtain confidential details or persuade victims to perform specific tasks.

Vishing attacks like its counterparts, heavily rely on social engineering methods in order to manipulate individuals into sharing personal information, carrying out financial transactions, or installing harmful software on their devices. The utilization of Voice over Internet Protocol (VoIP) technology simplifies the process for attackers to disguise their caller IDs and impersonate legitimate organizations.

Twilio's Compromised Accounts

On August 7, 2022, Twilio released a blogpost about an Incident report dealing with a smishing campaign by attackers which compromised some employee and customer accounts.

Upon completion of the investigation in October, Twilio also concluded that 'the same malicious actors likely were responsible for a brief security incident that occurred on June 29, 2022'. The employee was social engineered through vishing to give their credentials and the attacker had access to customer information for a brief period. Twilio said the threat actor was removed within 12 hours of identification.

Mitigations

After those intriguing stories you might wonder, 'How can I protect myself?'. Here are some tips:

Exercise caution with text messages

Be careful with unfamiliar or suspicious text messages, avoid clicking on links, and never share sensitive information via text.

Verify phone calls

Beware of funny phone calls requesting personal or financial information, try to verify the caller's identity, and avoid providing sensitive details unless certain of their legitimacy.

Be cautious with emails

Exercise caution when opening emails from unknown senders or those that seem suspicious, verify the sender's email address, and refrain from clicking on suspicious links or attachments. Spelling mistakes are always a dead give-away.

Strengthen passwords

Regularly update and maintain strong, unique passwords for your online accounts to minimize the risk of unauthorized access to personal information. This is just in case you have accidentally given away personal information.

Stay informed and educated

Stay updated on the latest tactics used in smishing, vishing, and phishing attacks, and familiarize yourself with common warning signs and red flags to better protect yourself from falling victim to such scams.

Conclusion

All three types of attacks aim to take advantage of people's weaknesses and trick them into compromising their security. To protect yourself, be cautious and sceptical of unexpected messages or calls. Verify the authenticity of communications, avoid clicking on suspicious links or sharing personal

information, and keep your devices and software updated with the latest security patches.

Happy Hacking 🙃.

Phishing Smishing Vishing Cybersecurity Mercurysnotes

Edit profile

Written by Daniel Iwugo

112 Followers · Writer for InfoSec Write-ups

Just another guy fascinated by the world of Hacking, Cybersecurity and the Internet. All my articles can be found here: flipboard.com/@elementmerc

More from Daniel Iwugo and InfoSec Write-ups