www.pwc.com/ng

Dealing with sophisticated phishing techniques

Cybersecurity and Privacy Monthly Bulletin

September, 2020

pwc

General Introduction:

This is a monthly Cybersecurity and Privacy update that focuses on key cyber security developments around the world with insights on lessons learnt and what your organization needs to do to improve cyber resilience and privacy.

The Netflix Phishing Scam

A few weeks ago, ArmorBlox, a cybersecurity company, reported a credential phishing attempt where phishing emails were sent to multiple customer inboxes with the aim of collecting personal information and payment card details. This phishing email impersonated Netflix Support, informing users of a billing problem due to a failure in verifying personal details.

The email claimed that the target's subscription would be cancelled if they do not update their details within 24 hours, furthering the sense of urgency. When targets clicked the link, they were led to a fictitious Netflix website with a phishing flow that asked them to input their login credentials, billing addresses, and credit card details. Once the phishing flow was complete, targets were redirected to the real Netflix home page.

Why was the attack successful?

The report from ArmorBlox provided a comprehensive analysis of the attack flow and why it succeeded:

1. The attack used a CAPTCHA page. CAPTCHA pages are usually used to prevent robots from using a website, and to confirm that a website is being accessed by an actual human being. This page served a dual purpose of giving the attack a look of legitimacy, and hiding the real page where the confidential information would be requested.

2. The web pages used to harvest confidential information were hosted on existing, legitimate websites, which had been earlier hacked and modified to include the web pages. The attacker likely used this to take advantage of the reputation of these existing domains, and avoid some security systems which might filter out unknown or low-reputation domains.

3. The web pages were carefully designed, to look like legitimate Netflix websites, including the right colors, logos, etc. This could create familiarity and a feeling of safety in anyone who views it.

Our Perspective

Phishing attacks have the potential to wreak havoc. Several phishing attacks have led to data breaches within prominent organizations in which millions of private user data (emails, addresses, credit-card details) have been made public.

The ubiquitous nature of phishing activities across the world is a matter of concern for most organizations, as users are being targeted with business processes they are familiar with, giving room for little or no verification of the authenticity of such processes. Organizations are advised to assist their employees in recognising phishing attacks being disguised as a normal business process.

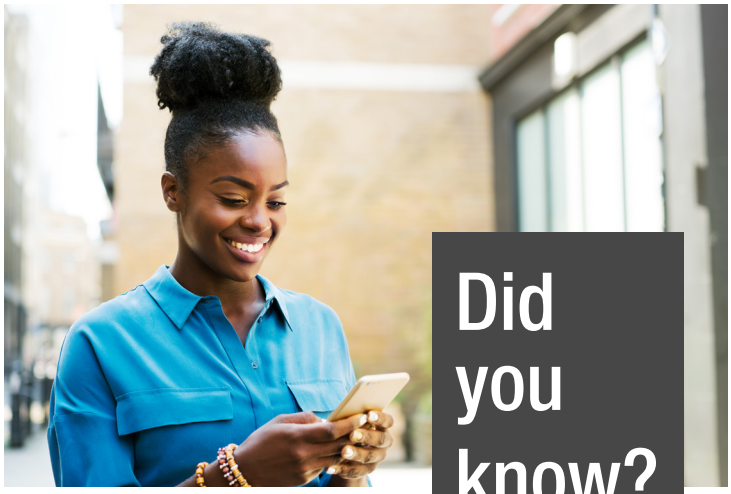
Mitigating Phishing attacks: What does this mean for you?

Malicious users can exploit poorly-designed processes to trick users into handing over information (including passwords), or making unauthorised payments. Organizations need to consider which processes could be mimicked by attackers, and how to review and improve them so phishing attacks are easier to spot and mitigate.

Furthermore, organizations need to also think about how the emails sent to suppliers and customers will be received. Questions such as “Can our recipients easily distinguish our genuine email from a phishing attack?” need to be addressed constantly as email recipients cannot be expected to look for and recognise every sign of phishing. Also, the provision of personal information cannot be used for identity verification as stolen or researched information is used by phishers to make their emails more convincing.

Here are a couple of ideas for mitigating the impact of phishing attacks .

- Ensure that staff members are familiar with the normal ways of working for key tasks (such as how payments are made), so they are better equipped to recognise unusual requests.
- Organizations should make processes more resistant to phishing by ensuring that all important email requests are verified using a second type of communication (such as SMS message, a phone call, logging into an account, or confirmation by post or in-person. Other examples of changing processes include using a different login method, or sharing files through an access-controlled cloud account, rather than sending files as attachments.



Did you know?

Many data breaches stem from phishing attacks.

Verizon’s 2020 Data Breach Investigation Report found that phishing is one of the top threat action varieties in data breaches, with 22 percent of data breaches involving phishing.

Source

https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

5 Questions for CISOs

1. Do your people have the skill and knowledge to detect phishing?
2. How secured and knowledgeable are your vendors and customers?
3. What exactly is the risk posed to my organization in the event of a successful cyberattack?
4. What are the top cyber threats facing companies such as ours today?
5. What is our company's response plan in the event of a successful cyberattack?

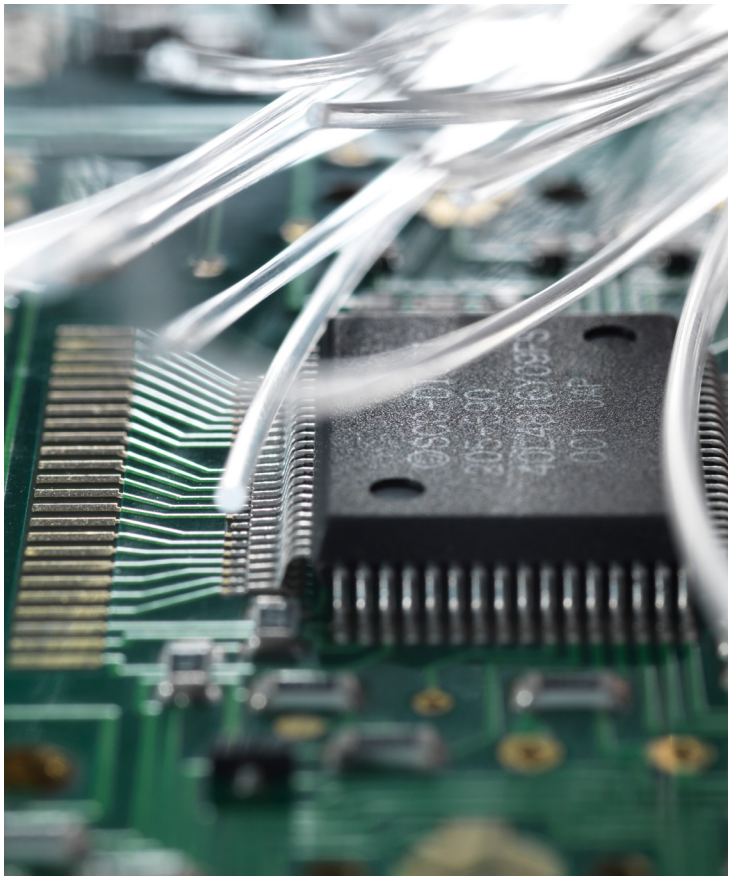
How PwC Nigeria Cybersecurity help business to create value:

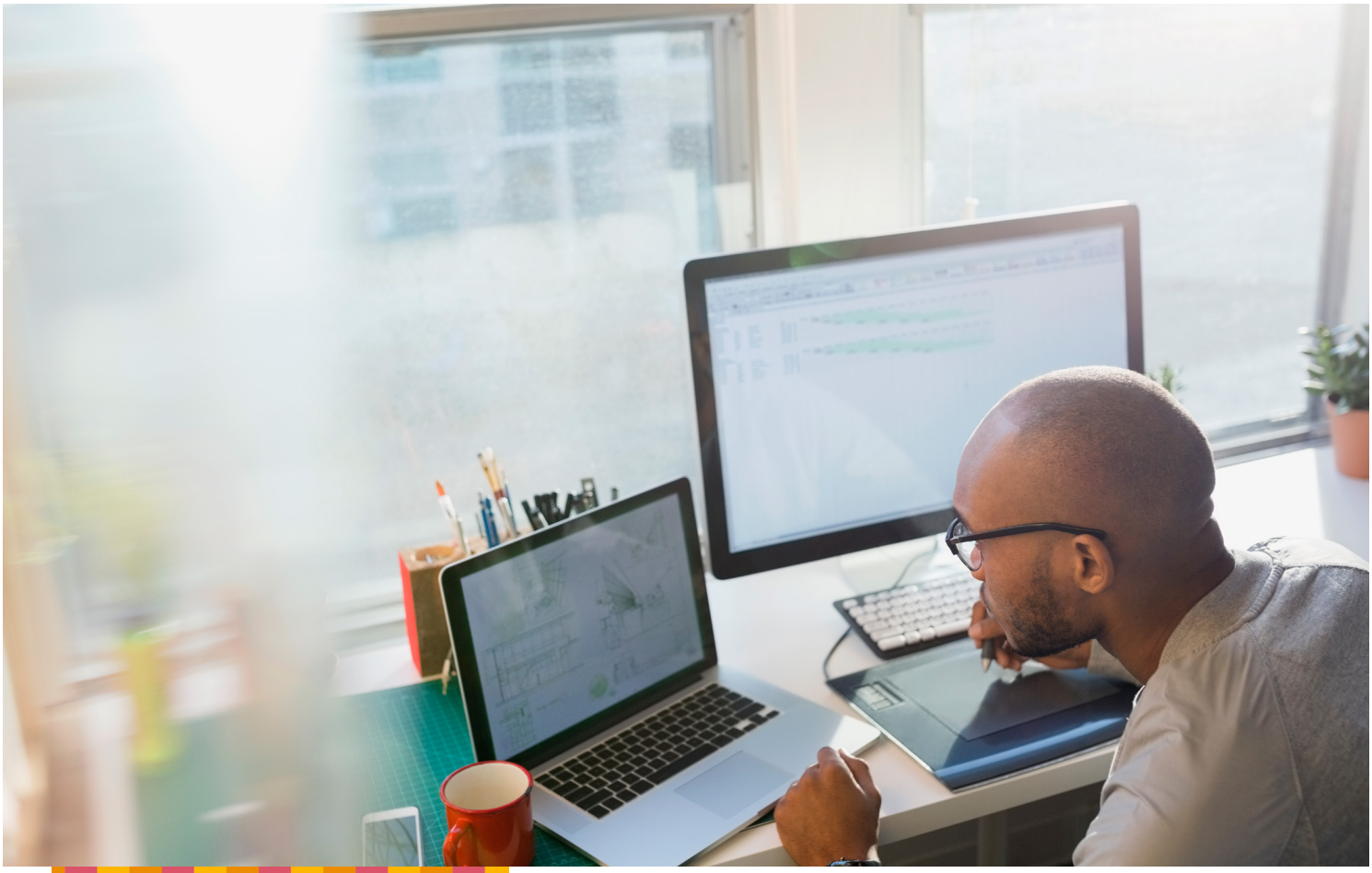
Our Cybersecurity and Privacy practice consists of dedicated professionals with significant business and technical expertise in helping top tier organisations to address complex business imperatives. We help clients secure their digital transformation initiatives, create organisational resilience, and derive risk and business value from data. We leverage the power of our global network to provide organisations with deeper, broader and timely expertise on evolving cybersecurity and privacy challenges.

We don't just protect business value, we create it – using cybersecurity and privacy as a tool to transform businesses.

Our services include:

- CISO as a Service (Virtual CISO)
- Cyber Resilience and Cyber Risk Management
- VMaaS, Cyber Penetration Testing and Application Security
- Compliance Management & Third Party Security Assessment
- Training & Awareness
- Cyber Risk Quantification





For more information, please contact:

Wunmi Adetokunbo-Ajayi
Partner Digital Risk & Cyber Security, PwC.
wunmi.adetokunbo-ajayi@pwc.com

Nkiruka Aimienoho
Senior Manager Cyber Security, Privacy & Resilience, PwC.
nkiruka.aimienoho@pwc.com

Chika Nwachukwu
Manager Digital Risk & Cyber Security, PwC.
chika.nwachukwu@pwc.com