FINANCIAL INVESTIGATION AGENCY
Advisory

01/2019 **11th November, 2019**

FRAUD ALERT
Advisory on Theft of Funds by Phishing

The Financial Investigation Agency (FIA) is advising the public to exercise caution when handling e-mails from seemingly legitimate companies. Cases of *account fraud* are increasingly being reported to the FIA. Thus far, a large amount of funds was stolen from several individuals' bank accounts in the Virgin Islands (British) through a type of social engineering tactic known as phishing.

Account Fraud

This type of fraud is predicated using a victim's sensitive data (passwords, personal identification numbers) to obtain credit, debit and bank account information. The perpetrator then uses the acquired information to make unauthorized transfers, charges or withdrawals from the victim's financial accounts.[1]

What is Phishing?

Phishing is the practice of sending fraudulent communication that appear to come from a reputable source.[3] It is usually carried out by emails but can also be conducted by text or instant messages. This scheme is designed to steal personal sensitive data from an individual (*identity theft*) to acquire bank account, credit or debit card information.

Identity Theft

When a criminal assumes another person's identity to benefit illegally from the victim. Once he or she has successfully assumed the victim's identity, they then use the personal information to commit fraud and other crimes.[2]

[1] 'ID Theft & Account Fraud: Prevention and cleanup', Consumer Action Managing Project, Consumer Action 2010. Accessed November 7, 2019.
https://www.consumer-action.org/english/articles/id_theft_account_fraud/
[2] Ibid., Consumer Action 2010.
[3] 'What is Phishing?' Accessed November 6, 2019.
https:www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

Advisory

How does Phishing Work

Phishing emails are often written in the form of a story. This tactic is intended to deceive you into clicking on a link or opening an attachment in an e-mail. Once the link or attachment is clicked on or opened, *malware* is then installed on your technological device allowing criminals to access your files and track what you are doing[5]. Armed with your financial information, the criminals then impersonate you and use the stolen information to conduct transactions directly from your bank or credit card account. This act is described as an 'account takeover activity'.[6]

Malware

Short for 'malicious software', is a computer programme designed to infiltrate and damage computers without the users' consent.[4]

Criminals are always working on improving their techniques, so the public is encouraged to be intentional about safeguarding personal sensitive data.

How to Detect Phishing Emails

The following are signs to help you identify phishing scam emails:

- The message is sent from a public domain such as "www.bancopopular@msn.com" instead of "https://bancopopular.com"
- The domain name is misspelled, for example, "www.poplar.com" as oppose to "https://www.popular.vi/"
- The email is poorly written using unusual phrases and grammatical errors
- The email includes suspicious attachments or links
- The message creates a sense of urgency[7]

What to Do If You Suspect a Phishing Attack

Don't:

- respond to requests made by phone or email for your personal information no matter the urgency. Always contact the bank to verify the legitimacy of the request.

---

[4] 'A definition of malware', BullGuard. Accessed November 11, 2019. https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification

[5] 'Phishing', Scamwatch, Australian Competition & Consumer Commission. Accessed November 6, 2019. https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing

[6] 'Account Takeover Activity', Department of the Treasury Financial Crimes Enforcement Network, December 19, 2011. Accessed November 6, 2019. https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a016

[7] Luke Irwin, '5 ways to detect a phishing email – with examples', IT Governance Blog, June 6, 2019. Accessed November 7, 2019. https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

- give personal information over the phone unless contact was initiated by you or there is absolute certainty that a representative of the bank is whom you're conversing with. [8]
- click on any links or open attachments in emails which claim to be from your bank requesting you to update or verify your information – just click delete.[9]

Do:

- search the internet for the names or exact wording of the email of message to check for references to a scam[10]
- periodically review your bank statements. Report any fraudulent charges/unauthorized transactions to your bank immediately.
- close compromised bank accounts, credit and debit cards immediately. Get account closures in writing from your bank.
- create new personal identification numbers and passwords for your credit & debit cards and your bank & e-mail accounts.
- shield your personal identification number while inputting it at ATM Machines or devices at supermarkets, restaurants or at any other local establishment. [11]

What to do if you are a Victim of a Phishing Attack

If you or someone you know have been the victim of a Phishing scam, whether the scheme was successful or otherwise, please contact your bank or financial institution immediately. Reports of phishing scams should also be directed to the police to the attention of Superintendent of Criminal Investigation, C. Alexis Charles, at The Royal Virgin Islands Police Force at 311 (BVI callers), 284 368 5371 (direct line) or 284 494 3822 (overseas callers).

Filing a report with the police does not absolve bank or financial institutions of their suspicious activity reporting obligations per Section 13 of the Anti-Money Laundering and Terrorist Financing Code of Practice, 2008, as amended. Reports must be addressed to the Steering Committee of the Financial Investigation Agency in care of the Director.

More Information

For more information on phishing, the public is encouraged to explore the websites listed in the footnotes of this Advisory.

---

[8] Ibid., Consumer Action 2010.
[9] Ibid., Scamwatch.
[10] Ibid., Scamwatch.
[11] Ibid., Consumer Action 2010.