THE SafeHarbor™ BRIEF

Gnostech Inc. *Maritime Cybersecurity Newsletter - May 2018*

COMBATTING COMMON USER THREATS

User Education and Awareness - PART 2

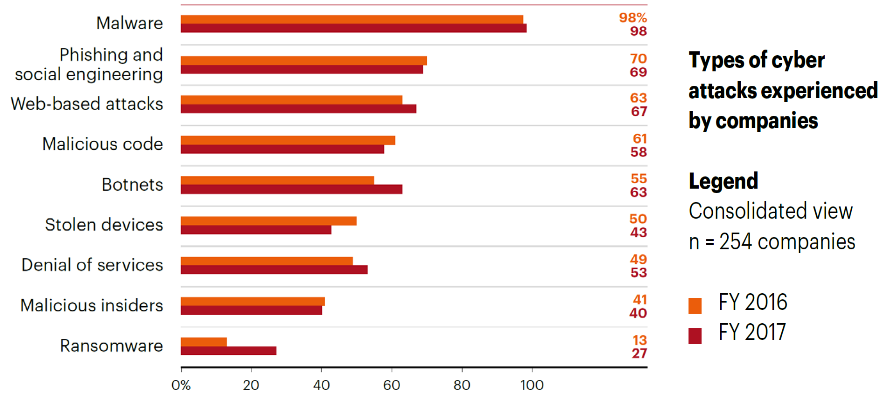
In the previous newsletter, we discussed the importance of user education and awareness as part of the methods to combat persistent cyber threats. This edition will educate users against one of the most common types of social engineering: phishing. Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Malicious actors will try any means necessary to gain access to your network, and your users are the first line of defense to protect your enterprise network. They will try to attack your users directly by using subterfuge and claiming to be someone your users can trust with their personal and network data by pretending to be a legitimate site, such as a bank, that the user may normally trust; or coerce users to visit malicious sites or download malicious applications by threatening their livelihood and pretending to be a government agency. What makes these attacks so successful, and dangerous, is that humans in general do not wish to get into trouble with their company or government.

Phishing

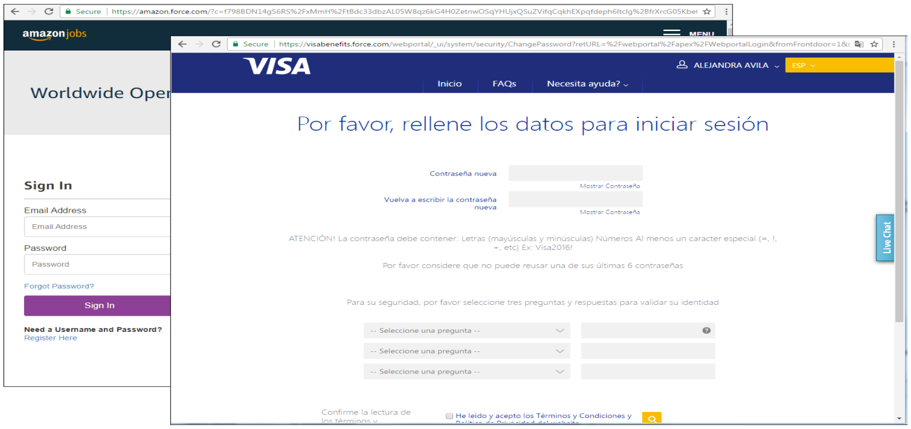
Phishing is the fraudulent practice of sending emails purporting to be from reputable companies to entice individuals to reveal personal information, such as usernames, passwords, and credit card details. Phishing is a form of social engineering primarily focused on deception through email communication with the goal of tricking users into believing the email has come from a reputable or trusted source. If you receive an important email from your bank stating you could lose your money if you do not click the link provided in the email, why would you not click on it? Most businesses will not send important or sensitive data regarding any user through an email. When in doubt, call the company directly instead of responding through an email.

Purpose of Phishing

Gain Sensitive Data – Attempts to trick a user into providing sensitive data about themselves or about their company. These types of emails will appear to come from a user's bank, utility company, etc., to get the user to provide their personal account data either through an email response or a fraudulent website provided in the email. Another example would be someone impersonating the company's helpdesk or security team in an attempt to gain access to their company network account.



Phishing is just one of the cyber attack methods used by malicious actors, according to Accenture's 2017 Cost of Cybercrime Study. Read the study to learn more: https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017


Secure
https://amazon.force.com/?c=f798BDN14gS6RS%2FxMmH%2FtBdc33dbzAL05W8qz6kG4H0ZetnwOSqYHUjxQSuZVifqCqkhEXpqfdeph6ltclg%2BfrXrcG05Kbe
amazon jobs
MENU
Worldwide Oper
Sign In
Email Address
Email Address
Password
Password
Forgot Password?
Sign In
Need a Username and Password?
Register Here
Secure
https://visabenefits.force.com/webportal/_ui/system/security/ChangePassword?retURL=%2Fwebportal%2Fapex%2FWebportalLogin&fromFrontdoor=1&
VISA
ALEJANDRA AVILA
ESP
Inicio
FAQs
Necesita ayuda?
Contraseña nueva
Mostrar Contraseña
Vuelva a escribir la contraseña nueva
Mostrar Contraseña
Live Chat
-- Seleccione una pregunta --
-- Seleccione una pregunta --
-- Seleccione una pregunta --
Confirme la lectura de los términos y
He leído y acepto los Términos y Condiciones y

Por favor, rellene los datos para iniciar sesión

ATENCIÓN! La contraseña debe contener: Letras (mayúsculas y minúsculas) Números Al menos un caracter especial (=, !, +, etc) Ex: Visa2016!

Por favor considere que no puede reusar una de sus últimas 6 contraseñas

Para su seguridad, por favor seleccione tres preguntas y respuestas para validar su identidad

PHISHING ATTEMPT EXAMPLE

This example shows a spoofed site that was sent to a user via email link. The site is fraudulent and is requesting the user's account information.

Install Malware to Company Network – Attempts to trick a user into downloading malware to their company or personal computer. These types of attacks will usually include an attachment or website link that will download malware to the system once it is opened or clicked on, and can come from what appears to be a trusted source, such as the company's helpdesk, security team, or HR personnel.

Common Features of Phishing Emails

Too good to be true – Exactly as it sounds, these deals seem too good to be true. Often these types of phishing attempts are designed to attract the user's attention through some type of monetary gain or prize. These emails will have a link or attachment that can be opened and will download a malicious application or software (malware) to your system. Remember the rule of thumb, if it seems too good to be true, it probably is!

Sense of Urgency – These types of phishing attempts offer deals or prizes that are limited in quantity or have only a limited amount of time left. They could also threaten the affected user with bogus legal action against them if they do not respond quickly to the email. These emails will also usually include a malicious link or attachment within the email for the user to click or open. The best practice for these types of emails is to report them to your cybersecurity personnel.

Attachments and Weblinks – Almost all emails with malicious intent will have some form of payload attached to them through either an attachment or hyperlink. Clicking on either of these can possibly load malware to your system. If you receive a suspicious email with an attachment or a link to a website, again report it to your cybersecurity personnel. Unknown Sender – If you do not recognize the sender of the email, it is best to delete the email.

Common Phishing Attacks

Spear Phishing – An attack constructed to appeal to a specific individual or group. For instance, an attacker could gain information on a specific user through Facebook or their LinkedIn account to create a more detailed phishing attempt against that individual (who they are, who they work for, hobbies, etc.)

Whale Phishing (Whaling) – A type of spear phishing attack that focuses on a high value target, such as a CEO or company board member. The account credentials belonging to a higher value target often offer a bigger payout for attackers. The primary goal for this type of target is to steal data and/or employee information for monetary gain.

Voice Phishing (Vishing) – An attack that uses a phone. Attackers will attempt to gain sensitive information about a company or individual through an automated call disguised as a user's financial institution. The message will request the victim to enter their bank account number and pin through the phone for identify verification. However, the malicious actor is stealing the information that the user entered in their phone to gain access to their bank account information.

Defense Against Phishing

The first and most important defense is user education and awareness. Test your users regularly to ensure they know not to click on unsolicited links or attachments and never provide their personal or sensitive information into a website without ensuring the site is trustworthy and protected! Implement spam filters, firewalls, and keep your anti-virus engines up-to-date. Consider blocking most pop-ups through your web browser. Always ensure when handling personal or company business transaction online, the site has the lock symbol to the left of the URL which ensures that the site is secured with HTTPS.

About Gnostech Inc.

Gnostech Inc. is an applied engineering and consulting company with over 35 years of experience and expertise in information assurance and cybersecurity engineering, and major combat and space systems development and integration. Gnostech provides the necessary knowledge and technology to ensure success of critical missions for customers in both the defense and maritime industries. To learn more, visit www.gnostech.com.