HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-04

CYBER ATTACKS TARGET HUMAN ERROR

1. Background:

Human error is central to social engineered attacks. Apart from the vulnerabilities in systems and applications, human error was commonly attributed to the success of cyber-attacks. Any personnel who have committed such may enable cyber-attacks to materialize. The vast majority of breaches result from inadequate security hygiene and lack of attention to detail and proactive stance in following cyber security procedures and protocols.

A general apathy exists and this leads to a 'wait and see' approach which more often than not, generates a reaction when it is too late. Organizational culture plays a crucial role in cyber security readiness and preparedness to defend against attacks by malicious actors. The importance of Cyber security needs to be cascaded down, most often handled by the ISO or ISNCO. Further, there needs to be a sense of accountability and ownership. Each personnel, military and civilian human resource needs to think 'safety-first' when faced, by an email, links, or invites of dubious nature.

Attackers are increasingly becoming sophisticated in their approach. Cyber security awareness training is a first step towards upping the level of knowledge in a workforce. Such training explains the various types of threats, the hacker's most common ways of attacking an organization and the consequences and impacts on the organization.

Policies are another key aspect in fighting or lowering human error that can lead to highly-negative consequences. Standards as to which official software to use, how to utilize company equipment, password management, authentication practices, updating security software such as antivirus software and firewalls, and connecting through secured WIFIs are common today.

2. Types of Human Error

Most studies and field-professionals categorize human errors in two categories, namely, skill-based and decision-based errors.

a. Skill-based human errors - employees would know the right course of action, but for reasons such as genuine mistakes or negligence, fail in accomplishing the action. The cause can be multifaceted, ranging from distractions, to over working leading to tiredness and lack of attention or distraction while carrying out a task or task list.

b. Decision-based errors - occur when a worker makes a faulty decision. Again, a number of factors come into play, such as not having enough information about a scenario or context or totally lacking the knowledge that they would not even realize what they are committing or leading to. In extreme cases, internal resources can be malicious in their behavior which would open cases of collusion with hackers.

3. **Recommendations**

In order to reduce human errors, organizations need to proactively strive to increase awareness by organizing cyber security awareness training and seminars; and sharing news and interesting informative reads on the intranet. Training increases knowledge. Choose training courses that emphasize on real life examples and scenarios, so that attendees can relate to and can easily understand and contextualize.

Clearly communicate policies and explain risks and potential consequences. Organizations are to have operating procedures in place that guide each personnel – such for example privilege control and password management. In addition to creating a secure environment, which proactively promotes cyber security best practices and ‘imposes’ security actions such as blocking pop-ups, black-listing certain shady URLs and auto-updating security software, promote security as an integral part of the organizational culture. Always encourage discussion, make escalation paths visible and easy to use, and hold training on a regular basis.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization’s overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit as a whole for educational, and non-commercial purposes.

Reference:

https://cybergateinternational.com/blog/cyber-attacks-target-human-error-improve-your-defences/