Volume 2 Issue 8

Date: 16.07.2025

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Cybersecurity is a constant evolutionary arms race

As long as humans continue connecting to the internet, they create security risks

In a rapidly changing landscape like cybersecurity, no one can claim to know everything all the time

Inside this Digest:

Quid Pro Quo Attacks

Quid pro quo attacks fall under the umbrella of social engineering frauds, where the attacker offers a service or benefit in return for information or access. Imagine someone posing as a tech-support agent offering to speed up your computer. They seem reliable and say all the right things to make you believe you need their services. In fact, they really help you speed up your computer, and you believe you received your side of the bargain. However, what if, in the process of speeding up your computer, they gain access to your sensitive files and steal your info? This is the deceptive give-and-take at the heart of quid pro quo attacks.

Anatomy of a quid pro quo attack

Recognizing quid pro quo attacks

While distinguishing a quid pro quo attack from a genuine offer for products or services can be challenging, some signs help you detect a quid pro quo attempt. If you notice any of the following, approach them with caution and reach out for help if needed:

Unsolicited offers or requests: One sign of a quid pro quo scam is the unsolicited nature of the offer or request. Remember that employers don't typically reach out to individuals with job offers out of the blue, and legitimate tech support doesn't magically appear at your doorstep. Similarly, valid medical solutions don't manifest without prior inquiry.

High-pressure tactics: Scammers are masters at creating a sense of urgency to make you act hastily without thorough consideration. You might encounter phrases like "This offer won't last long," "Other buyers are waiting to cash in," "Many candidates have already applied," or "We only have a limited number of positions available."

Requests for personal or financial information: Since quid pro quo scams often appear to involve a fair exchange, requests for personal information can appear discreet and necessary. Watch out for demands that deviate from the ordinary, such as requests for your social security number or bank details. Legitimate transactions rarely require such sensitive information upfront.

Unclear or unrealistic promises: The age-old adage "if it seems too good to be true, it probably is" applies perfectly to quid pro quo scams. Whether it's a miracle cure, a get-rich-quick scheme, or a job that promises substantial returns with minimal effort, these unrealistic offers should trigger your skepticism. They are often traps designed to deceive you into providing fraudsters with information or money.

Suspicious payment requests: Financial matters should be transparent and reasonable. If a potential service provider suddenly requests payment for services, training, or equipment you haven't requested or they haven't provided, it should raise a red flag. Be careful with unspecified and unexplained payment requests and ensure that such transactions have been previously authorized.

The human element: Why we fall for quid pro quo scams

The success of quid pro quo attacks is mainly due to psychological manipulation techniques that are used by attackers. By offering to do a favor or help, attackers create a sense of indebtedness in the target, making them more likely to comply with their requests. This is further reinforced by the principle of reciprocity, which is deeply ingrained in human behaviour.

In these scams, attackers often impersonate trusted authority figures or experts, making it easier for them to gain the trust of their targets. This can be in the form of impersonating, for example, an IT support person or a customer service representative. Individuals are more likely to trust and comply with the requests of someone they perceive as an authority figure.

In addition, attackers may also create a sense of urgency in their targets by using tactics like time-sensitive offers or threats. This can make the target feel stressed and act quickly without thinking things through, making them more vulnerable to falling for the scam

Digital hygiene: Fortifying against quid pro quo attacks

While there is no guarantee against quid pro quo attacks, chances are you are more likely to detect and not act upon them if you apply a set of security best practices. Here are some things to improve your digital hygiene and help you to recognise and deter quid pro quo attacks:

Employee training: Educate your staff about the dangers of quid pro quo attacks and provide clear guidelines for identifying and responding to potential threats. Regular and continuous training sessions can reinforce their awareness and vigilance

Robust authentication: Implement strong authentication measures to verify the identity of individuals requesting sensitive information or access. This can include multi-factor authentication (MFA) and verification procedures

Comprehensive security policies: Develop and enforce comprehensive security policies that outline how sensitive data should be handled, shared, and protected. Ensure your employees are aware of and follow these policies

Incident response plan: Prepare for the worst by creating an incident response plan that outlines the steps to take in the event of a security breach. Timely action can minimize the damage caused by an attack.

Regular monitoring and assessment: Continuously monitor and assess your organisation's digital security posture. Regular security audits can help identify vulnerabilities and areas for improvement.