Information Security Awareness

Phishing Awareness Remediation Procedure

BRG IT Cybersecurity periodically conducts security awareness phishing campaigns. A phishing awareness campaign is a structured effort to educate our colleagues within BRG about the dangers of phishing attacks and to provide them with the knowledge and tools to recognize and avoid falling victim to such attacks. Phishing is a fraudulent attempt to obtain sensitive information, such as usernames, passwords, and credit card details, by disguising oneself as a trustworthy entity in electronic communication. These attacks often come in the form of deceptive emails, text messages, or websites.

Here's why having a phishing awareness campaign is crucial:

- **Protection against Cyber Threats**: Phishing attacks are one of the most common and effective forms of cyber threats. By educating personnel about phishing tactics and warning signs, organizations can significantly reduce the risk of successful phishing attacks.
- **Safeguarding Sensitive Information**: Phishing attacks can result in the compromise of sensitive data, leading to financial losses, reputational damage, and regulatory fines. A phishing awareness campaign helps personnel understand the importance of safeguarding sensitive information and how to handle it securely.
- **Preservation of Trust and Reputation**: Falling victim to a phishing attack can damage BRG's reputation and erode trust with clients, business partners, and stakeholders. By preventing successful phishing attacks, BRG can preserve trust and maintain their reputation.
- **Compliance Requirements**: Our clients and their related industries have regulatory requirements for data protection and cybersecurity. Implementing a phishing awareness campaign helps BRG demonstrate compliance with these requirements and avoid potential legal and financial consequences.
- **Empowering Our Colleagues:** Our personnel are often the first line of defense against phishing attacks. By empowering our colleagues with the knowledge and skills to recognize and report phishing attempts, BRG can create a culture of security and strengthen their overall cybersecurity posture.

Overall, a phishing awareness campaign is essential for mitigating the risk of phishing attacks, protecting sensitive information, preserving trust and reputation, meeting compliance requirements, and empowering employees to defend against cyber threats.

IT Cybersecurity maintains records of repeat offenders participating in these phishing campaigns. To address and correct the behavior of repeat offenders, IT Cybersecurity has implemented the following remediation levels for these colleagues:

- **1St Breach** - A splash screen informing the colleague that this was a phishing awareness test and instructing them of what was wrong with the message.
- **2nd Breach** - The colleague is moved into a group that enforces multifactor authentication every 24 hours, instead of every 30 days, until an advanced phishing awareness training course is taken.
- **3rd Breach** - The colleague is moved into a group that enforces multifactor authentication every 24 hours until the individual passes 4 consecutive (1 year) phishing campaign training emails. Additional phishing training will be mandated, Human Resources and the colleague's manager and / or community leader will be notified, and the infraction will be noted in the employee's file.
- **4th Breach** - The colleague is moved into a group that enforces multifactor authentication every 24 hours permanently and further disciplinary action will be taken by Human Resources, up to and including termination.