DUBAI, UAE 2021.

When something is “phishy”: what you need to know

gbmme.com

When something is “phishy”: what you need to know

As more organizations reopen their office spaces to welcome back employees, many professionals are receiving emails containing status updates about the safety protocols.

While the bulk of these messages are legitimate, many employees receive dubious emails which mimic the aesthetic of their company’s messaging system or HR department. These phishing emails often ask employees to confirm the receipt of the message as soon as possible, with a completed form and their personal identifiable information.

Considering that organizations have been sending similar types of emails since the outbreak of COVID-19, it is easy to see how users can mistake phishing emails for the real thing.

So, what exactly is happening?

Phishing: A fraudulent cyber practice

Phishing is based on sending fake communications, usually emails, which are designed to look like they’re coming from a trusted source. Attackers send messages in order to steal sensitive user data, such as login credentials, passwords and credit card numbers, or install malware on the recipient’s computer. When hackers target a company, the results can be costly and devastating.

Today, phishing attacks account for more than 80% of reported security incidents . Using individuals’ personal identifying information to make unauthorized purchases and steal funds, attackers often use phishing as a gateway to bigger cybercrime attacks, including ransomware and advanced persistent threats (APTs). Gartner predicts that, through 2023, business email compromise (BEC) attacks will continue to double each year to over $5 billion and lead to large financial losses for enterprises.

Top 4 common types of phishing attacks

Deceptive phishing is the most frequent type of attack. The attackers' goal here is to obtain confidential information from their victims in order to steal their money. It's usually done by asking users to click a link or check their account details.

- *https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats——-what-you-need-to-know-for-2021/?sh=5e07f9258d3d*
- *Protecting Against Business Email Compromise Phishing, Gartner, 2020*

Pharming is a method of directing users to a fake website that can compromise their computer or the DNS server software. Users don't need to click the link to be sent to the fraudulent site.

Spear phishing is targeted towards a specific individual after criminals profile their victim online. It's often the first step attackers take to evade the defence system and infiltrate an organization.

Whaling is the practice of aiming for the "big fish," such as a C-suite executive. Usually, hackers invest significant amounts of time to unearth information about their prey and find the right time to strike.

How should companies raise employee awareness of phishing attacks?

User training is the most effective way of alerting employees to phishing. Training workshops should be designed so they address all employees in the organization, although executives tend to be more common targets. Training materials should focus on teaching employees how to spot a phishing email and what measures to take once they receive it. Simulation exercises are another great tool for companies to assess the vulnerability of their employees to staged attacks.

Additionally, organizations need to let their employees know which internal department is responsible for sending official "back-to-office" related emails and other status updates. They

should advise their employees to treat any emails of this type from other sources with suspicion and provide a contact email in the event that they receive such communications.

How can you protect yourself as an end-user?

- **Watch out for notifications** demanding urgent action. This tactic is devised to intimidate recipients into making an erratic move. Promises of lucrative prizes that you must claim before they're gone, or warnings of having your accounts closed unless you provide confidential information, are only a couple of examples.
- **Inspect the link for inconsistent URLs**. Phishing methods regularly use legitimate-looking domains. Bad spelling or a mismatch between addresses in the body of the email and the target address is a red flag.
- **Pause before clicking links and downloading files**. Sometimes, all that's needed is a momentary lapse in judgment to take the bait. Scrutinize sender information to make sure it's safe to proceed with your activity.

Conclusion

In the battle against phishing attacks, employees are every organization's first line of defence. That's why companies need to invest in educating their staff to recognize these attacks in a timely way. When people are empowered to successfully handle security challenges, they'll know better than to respond to emails from a Nigerian prince or a long-lost friend who popped up to ask for money.

For any questions you have regarding phishing attacks, GBM Application Security experts are here to help! Reach out to us at ask@gbmme.com.