Phishing

The Biggest Security Threat Facing Businesses

Phishing email attacks are one of the greatest security threats businesses face today. These attacks are hard to detect and extremely profitable for cyber criminals.

91% of cyber attacks on businesses begin with phishing.[1]

65% growth in phishing emails occurred over the past year.[2]

97% email recipients failed to distinguish a phishing email from a legitimate email in test exercises.[3]

90% odds an attacker will succeed in fooling one employee if they send out 10 phishing emails.[4]

Types of Phishing Schemes

Phishing is so profitable it has proliferated into multiple forms of attack:

Deceptive Phishing
Targets: All employees
Attack Vehicle: Emails with malicious links
Seeks: Login credentials or financial data, or to deliver ransomware
Variations: Vishing (by phone) and smishing (by SMS text)

Spear Phishing
Target: Specific employees (executives, finance, HR)
Attack Vehicle: Highly personalized emails and fake websites
Seeks: Login credentials, financial data, or to deliver ransomware

Whaling
Targets: CEO and the Board
Attack Vehicle: Well-researched, tailored email and fake websites
Seeks: Highest security level-access to systems

Business Email Compromise (BEC)
Targets: Finance and accounting employees
Attack Vehicle: Your internal email system—impersonating the CEO or CFO
Seeks: To trick other financial employees into initiating bank transfers

Pharming
Targets: All employees
Attack Vehicle: DNS cache poisoning redirects browser—no link needed
Seeks: Login credentials or financial information

Think Before You Click!

The more you train employees, the more careful they will become. Follow these tips to safeguard your business by encouraging them to:

1. Inspect URLs and only login to HTTPS websites.
2. Check the sender line carefully.
3. Watch for strange spelling or grammar.
4. Be wary of attachments and links.
5. If in doubt, call—don't click.
6. Train employees—even the CEO.
7. Run real-world exercises.
8. Use two-factor authentication.
9. Report suspicious emails quickly.
10. Add another line of defense with cyber monitoring.

[1] "2016 Enterprise Phishing Susceptibility and Resiliency Report," Cofense.
[2] "2017 Enterprise Phishing Resiliency and Defense Report," Cofense.
[3] "Intel Security Study," 2015.
[4] "2017 Breach Investigations Report," Verizon.