Addressing your CYBER SECURITY THREAT

b/net SYSTEMS

Cyber security threats have two main targets: technology and technology users. The human component is often neglected, yet in the business world today, phishing, spear phishing, and business email compromise present the greatest cyber security risks. As a result, your employees are the first line of defense against damages to your organization. The more your staff are aware of the vulnerabilities and how to protect themselves, the stronger your organization's human "firewall" against a cyber security attack.

Facts and Figures

✓ Phishing is still the most commonly used attack on organizations, with 75% of cyber attacks coming from outsiders.[1]

✓ Phishing attacks were up 297% from Q3 2017 compared to that same period in 2018.[2]

✓ 1 in 100 emails is now a hacking attempt sent with the goal of compromising a user or network. Just one malicious email can provide attackers a route to significant damage.[3]

✓ About 57% of small- and mid-sized businesses experienced an increase in cyberattacks in the last 12 months, and the majority expect that trend to carry through into 2019.[4]

✓ 2018 saw a 500% increase over last year in ransomware attacks on Mac and iOS devices.[5]

✓ Organizations are only "moderately ready", on average, to handle cyber security-related threats.[6]
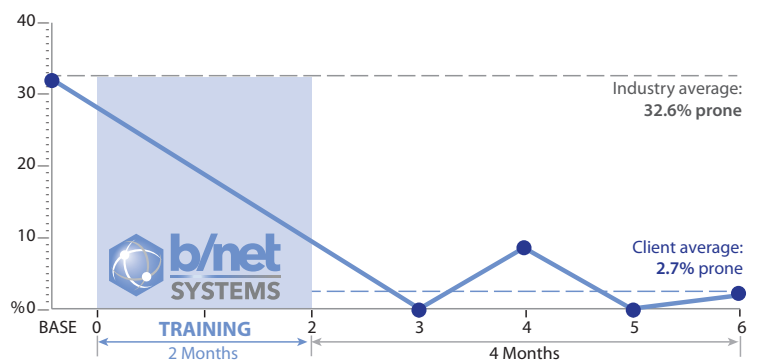
BE PREPARED: Cyber Security Training

B/Net, in partnership with an industry leader, offers an effective and measurable cyber security training program. Using our online platform, we safely phish your organization to determine how prone your business is to a cyber security attack. We train your staff to recognize cyber security threats and continue to measure improvements against a baseline. B/Net provides data to show our program brings you value and peace of mind.

— CASE STUDY —

Our training process has demonstrated success in significantly improving phishing awareness. A mid-sized association's recent B/Net cyber security training resulted in a **91.7% phishing proneness improvement**.

• Prior to training, their baseline phishing proneness score was 31.9%; the industry average is 32.6%.

• After training, we measured phishing proness at 30-day intervals for 120 days. The average phishing proness across these 4 tests fell to 2.7%.

• The great majority of staff are now able to recognize and ignore phishing emails.

CYBER SECURITY TRAINING EFFECTIVENESS

Procure B/Net's cyber security training today by contacting Chris Dean at info@bnetsystems.com.

[1] 2018 U.S. State of Cybercrime, IDG, [2] The Retail and eCommerce Threat Landscape Report, October 2018, Intsights Cyber Intelligence and Riskified, [3] Email Threat Report, 2018, FireEye
[4] The 2018 State of Endpoint Security Risk Report, sponsored by Barkly, independently conducted by Ponemon Institute, [5] Global State of the Channel Ransomware Report 2018, Datto
[6] IT Trends Study 2018 Comprehensive Report, November 14, 2018, Society for Information Management (SIM)