NTT Security

Five tips to prepare your organisation for a planned phishing simulation exercise

As phishing attacks become more sophisticated and difficult to detect, running a **phishing simulation exercise** is a key component of many organisations' Security Awareness training programmes. It can quickly and efficiently highlight the dangers of cybersecurity threats and help you assess the effectiveness of training undertaken by employees.

See below NTT Security's top tips for planning a phishing simulation exercise for your business.

Raise security awareness on the boardroom agenda

Ensure management understanding and buy-in to the phishing attack simulation. Invest time to make management aware of the risks and potential consequences of a successful phishing attack and the impact on your business, which can be triggered by a simple click on a link in a phishing email.

Communicate with all stakeholders

Before you begin a phishing simulation exercise, ensure all stakeholders are informed. Depending on how your organisation works, this may extend to involving unions and Human Resources, to ensure that all stakeholders understand why the phishing simulation exercise is needed. A phishing test does not aim to expose individuals, but looks to identify factors that may constitute a security risk for the business.

Perform regular phishing simulation exercises

Phishing simulation exercises are simple to perform and require minimal input from your employees. By carrying out the testing on a regular basis, and by sharing the results, you can track and reward progress, and uncover new areas of risk as they arise. Regular testing also helps keep phishing attacks at the forefront of employees' minds.

Identify areas for improvement

Use the phishing simulation exercise report to identify areas of highest risk and priorities and select counter measures based on these findings.

Provide adequate and ongoing training

It's important to maintain the focus on phishing between the planned simulation exercises. Make sure employees understand what characteristics and warning signs they should look for to detect a potential phishing attack. Some phishing is now so sophisticated that employees can be convinced that a request has been sent from management, or other trusted contacts. It is important that your employees know the warning signs and remain vigilant.

About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.

NTT Security

www.nttsecurity.com