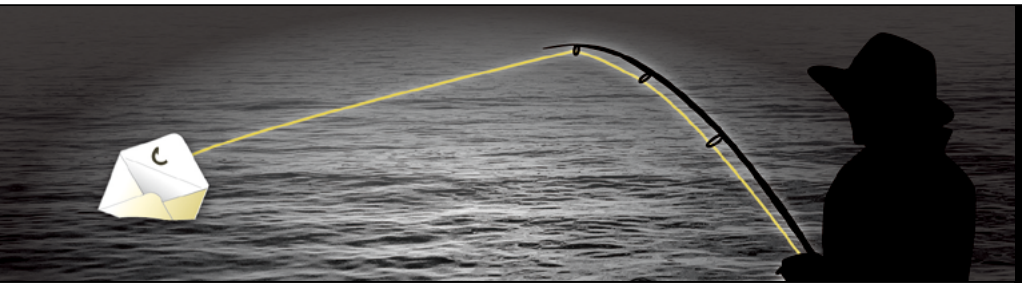
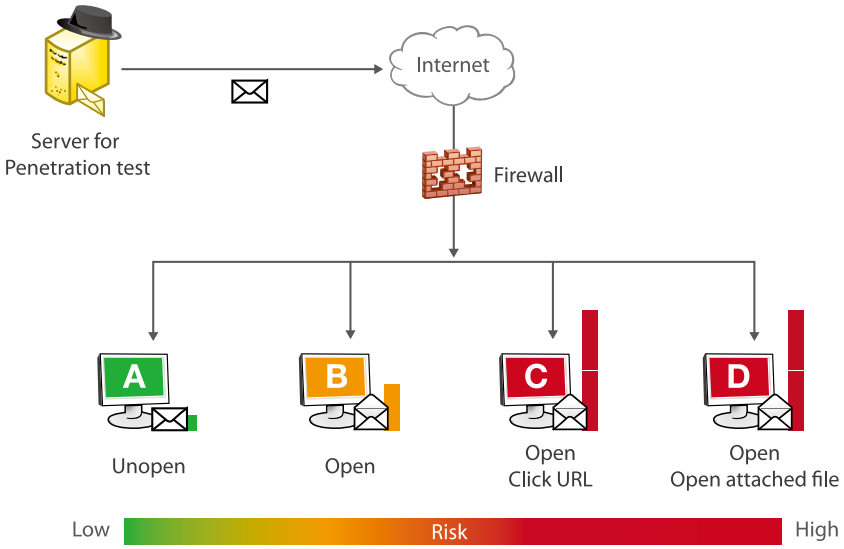


Strengthen internal security awareness. Provide top notch IT consulting services.

Penetration Testing Services

Social Engineering is a phishing attack where a hacker takes advantage of the curiosity and negligence of users to steal valuable information of the person or an organization. It has become a trending vulnerability in corporations and government institutions. Penetration Testing Services educates your staff to practice safe e-mail habits. We also analyze potential risk and give suggestions for improvement.



One of the most common forms of social engineering is through the use of email phishing attacks. IT personnel can spend time and effort implementing firewalls, IPS, email gateways and end-point security and ironically, people are still one of the easiest vulnerabilities attacker uses. A hacker only needs as little as a message promotion coupon to completely compromise a company reputation.

The Penetration Testing Services creates a benchmark on the organization's vulnerability. This services is designed based on the statistics results, thus it improves the employees' awareness and vigilance of their daily email habits.

Because it is important to control the level of awareness among them, Cellopoint emulates a real-world phishing campaign by creating a situation similar to an actual hacker. This provides a better insight of your employees' behavior. You can create customized test template and flexibly decide sending time and date.

To give you an accurate reading of the level, we record the email accounts of those who visited the malicious test site or downloaded the attachment, and categorize them as none, low or high security risk. After the test, all your employees will have good email habits, and thus the risk of being attacked goes nearly to 0.

Features

- Decrease the possibility of being attacked from hackers, by raising employees' awareness.
- Analyze internal security vulnerability
- Deliver professional technical counseling and guidance
- Provide statistics on your employees performance

Cellopoint®
Secure Your Email

Methodology

1. Request for Penetration Testing Services

If you have any threat experience or preliminary indications, contact one of our CelloConsult representatives and share with us your current situation. This will help us to develop and personalize a scenario appropriate to your organizational culture.

2. Determine the Scenario

We work jointly with you to develop the suitable scenario, preferred timing, and create customized emails similar to the ones designed by social engineering hackers, according to your staff lifestyles.

3. Create Email Template

These emails could be related to gossips, elections, stock investment, or any breaking news, and includes text, image, links and attached files. Other type of template redirects users to another website and induce them to disclose sensitive information such as usernames and passwords.

4. Prepare the Attack

You still have a business to run, so it's important to make sure mail system is working properly and carry the attack through a time when employees are not in training or another activity.

5. Run the Test

Tests are taken place without any advanced notice to any department, using a floating IP e-mail templates.

6. Collect the Results

Once the test is concluded, we gather the performance results of all employees and present it in an unified report. This reveals the test results, including details about the employee's name, department, test results, the email open rate, click-through rate, and file download counter:

1. The employees who did not open the email have no risk.
2. The ones who open the email are shown as low risk.
3. The employees who open and click URL link or download the attached file are marked as red, treated as high risk for the organization security and assessed accordingly.

The test results and private information are kept confidential, in compliance with the Personal Information Protection Act.

7. Advise your Employees

If the manager approves it, after the test is closed, the results will be sent automatically to each participant. This saves time to IT administrator on talking to employees separately about the importance of his or her security awareness.

8. Provide Recommendations.

At the end, you will get comprehensive statistics and the performance report of each user. You can see which department is more vulnerable and advise your staff personally. We suggest appropriate actions to be taken in order to improve the security of your network.

Benefits

- Reduce the risk of data leakage
- Promote healthy email habits.
- Demonstrate organization's commitment to data security
- Enhance internal awareness of information security
- Reduce the burden of IT staff to focus in other projects.