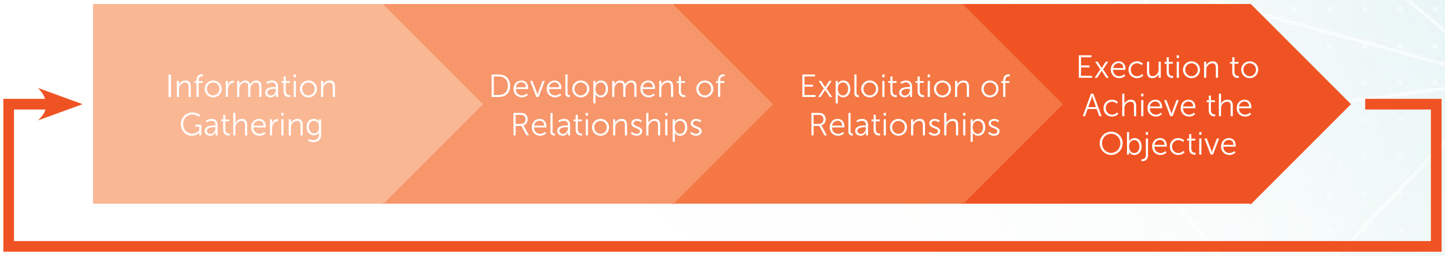
Phishing Simulation Risk Assessment

Phishing attacks are designed to deceive individuals into providing sensitive information such as passwords to a malicious third-party, or into performing actions such as downloading malware designed to give an attacker remote control over the victim's computer. Disturbingly, these attacks are becoming increasingly sophisticated, to the extent that often neither the individual nor the organization to which they belong is even aware that an incident has occurred until it is too late.

THE SOCIAL ENGINEERING ATTACK CYCLE


Information Gathering
Development of Relationships
Exploitation of Relationships
Execution to Achieve the Objective

Do you really know your security posture?

To gauge your current security posture in terms of the risk posed by phishing attacks, ask yourself the following questions:

- As part of your regular security assessments, have you ever performed a controlled phishing attack?
- Would you expect your employees to click on a malicious link within an email? Would they then go on to disclose authentication credentials or attempt to download a malicious payload?
- How many employees in your organization would you expect to perform those actions?
- Which offices and departments within your organization are most likely to be susceptible to a phishing attack?
- Therefore, do you know where your security training budget is best spent for maximum impact and 'quick wins'?
- Have you ever run security awareness campaigns? If so, how effective do you think they were?
- If there were a phishing attack, would there be an internal response, or would it go unnoticed?
- Is the response guaranteed to go as per policy and procedure, or would a real world attack be likely to cause chaos and confusion?
- If there were a response, would it be sufficient to mitigate the risk posed by the attack?
- Is your organization more or less susceptible to phishing attacks than other organizations within the same market sector?

AURORA

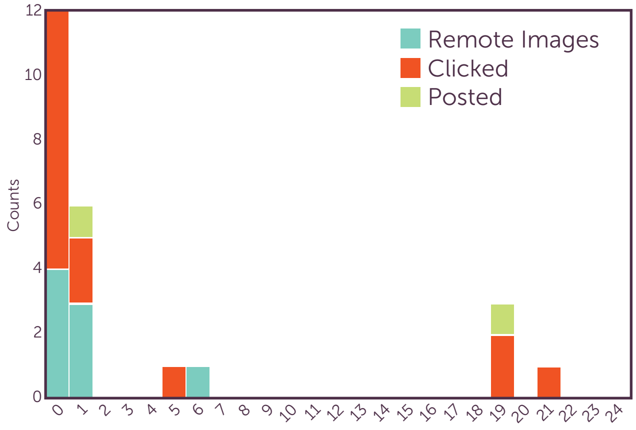
Phishing Simulation Risk Assessment

Aurora's Phishing Simulation Risk Assessment measures the current level of susceptibility by performing a controlled attack against employees. Such an attack typically targets a subset of employees from each department within the organization. If appropriate, employees and departments from different offices are also be included within the test, in order to allow for the identification of any trends across the entire organization.

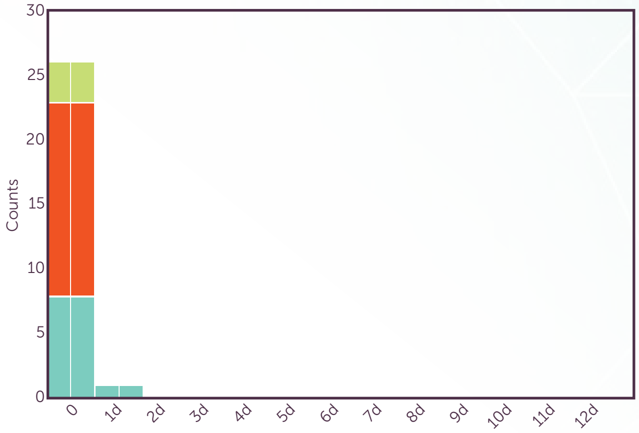
The data returned by such an assessment is invaluable in gauging current levels of susceptibility and providing information such as:

- Number of users who clicked a malicious link within an email
- Number of users who entered corporate domain credentials into a phishing website
- Number of users who attempted to download a malicious executable
- Breakdown of susceptible employees into various demographics, such as office, department or location
- Activity over time (were users still clicking malicious links even after the internal security response?)
- Use of weak passwords within corporate domain credentials
- Did any employees reply directly to the phishing attack?
- Comparison against the average susceptibility of other organizations in your market sector

ACTIVITY IN FIRST 24 HOURS



ACTIVITY IN ENTIRE CAMPAIGN



Once a baseline has been established, strategies for mitigating risk are investigated and implemented. There are a number of approaches that, when combined, are extremely effective in dramatically cutting the overall level of susceptibility.

Ready To Get Started?

Contact us at 888-282-0696 or sales@aurorait.com to learn how Aurora Security Services can help you accomplish your specific business and IT security goals. Explore further by visiting our website at: www.aurorait.com