context

Phishing Assessments

Malicious phishing attacks are an increasingly common threat and are often the first step in the majority of real-world compromises. Regular and controlled phishing assessments allow organizations to measure their exposure to attacks that seek to deliver exploits or extract user credentials. A phishing assessment provides assurance around both the technical controls and user awareness that are needed to prevent key assets from being compromised.

Why Context?

We draw on our experience of performing real-world phishing attacks in red team engagements, as well as insights from responding to attacks against our customers.
We can also provide corporate training programmes in conjunction with regular phishing assessments to raise awareness with end users around the dangers of phishing and allow them to develop their capability to spot malicious emails.

How we can help:

- Send simulated phishing emails to your employees/users in a controlled manner
- Design a range of targeted phishing emails varying from mass-emailed messages to highly targeted emails
- Safely track user actions - in an anonymized way, if required
- Redirect users who clicked on a phishing link to an e-learning platform to provide immediate awareness education
- Assess technical controls in place to protect against spam and phishing emails
- Benchmark user awareness and trends that can be analyzed across regular assessments
- Provide corporate training programmes to raise awareness with end users

Process

Context's approach to delivering phishing exercises typically comprises the following phases:

Staging

The first phase of an exercise is the staging phase during which Context creates and prepares a phishing campaign or a series of phishing campaigns tailored to your organization's requirements. Depending on the level of sophistication required, Context can set up a range of targeted phishing attacks, varying from mass-emailed messages to highly targeted emails aimed at a small group of users. Context's experienced consultants devise emails that users may access, but that do not raise suspicion or have undue side effects. The phishing emails designed will typically be modeled on real-world techniques, including 'spoofed' email addresses, filter evasion, manipulating links to hide the real target and supplying attachments containing (simulated) malware.

Execution

All campaigns will be delivered by Context's unique automated phishing platform 'CPhish', which has been developed to effectively craft and track phishing campaigns and can provide a statistical breakdown of the number of users accessing links or files, mapped against the specific campaign used.

E info@contextis.com
T +1 917 880 3130

context

Phishing Assessments

Each email contains an individual link or attachment allowing users to be tracked, either by their real names, or in an anonymized way if required by the data protection legislation in place within the country in which the campaign is being performed.
The payloads used by Context are designed to profile the user in a safe and non-intrusive way and can be configured to redirect the user to a phishing awareness training platform in order to provide immediate awareness education, if required.
Context are furthermore able to assess an organization's technical controls by sending targeted emails containing a range of common attack payloads from 'spoofed' and genuine email addresses, hence testing the strength of email filtering and malware detection capabilities in place. We can also identify whether a user is running a vulnerable browser or common plugins.

Analysis and reporting of results
Upon completion of the engagement, Context will provide a detailed report including the overall results of the assessment as well as statistics and analysis around the success of the campaign. This can include information about the rates of users accessing links or files and the percentage of users whose web browsers or computers are vulnerable to publicly-known vulnerabilities.
Context also offer optional user awareness workshops that can be held prior to or after a phishing campaign to further test and strengthen security awareness.

E info@contextis.com
T +1 917 880 3130