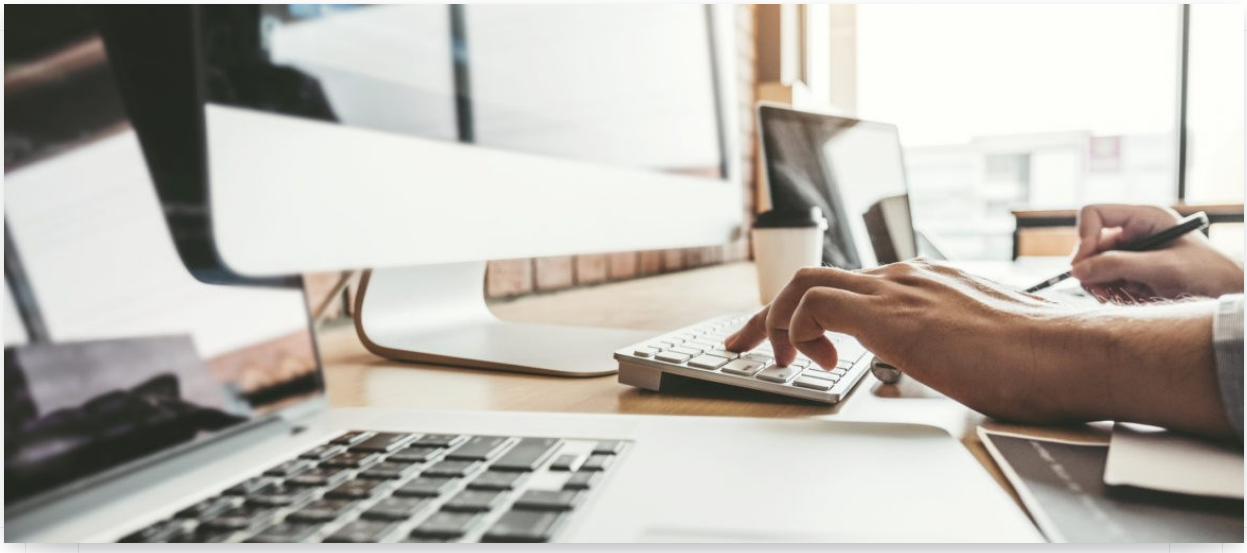
Debevoise & Plimpton | Data Blog

CYBERSECURITY

Phishing Testing for Employees—What To Do with Those Who Fail?

BY: AVI GESSER, JEREMY FEIGELSON, TRICIA SHERNO, CHRISTOPHER GARRETT, STEPHANIE CIPOLLA AND JOSE ANGEL LAMARQUE III - JUNE 25, 2020



As many people return to their workplaces, cybersecurity attacks continue unabated. Email phishing remains the most common method by which cybercriminals first gain unauthorized access. These phishing attacks can then lead to ransomware incidents, business email compromise scams and other destructive cyber attacks. So, training employees to be able to spot phishing emails is as important as ever, as is testing, to make sure that the training is effective. Indeed, training is increasingly a legal requirement and many leading cybersecurity regulatory frameworks also require phishing training for employees (*e.g.*, International Organization for

Standardization/International Electrotechnical Commission information security standard ISO 27001 Clause A.7.2.2), but they offer no guidance on what to do with those who fail. In this Debevoise Data Blog post, we discuss companies' remedial options for employees who fail phishing tests and when each may be appropriate.

Employees Who Repeatedly Fail Phishing Tests May Create Risk

Phishing testing most commonly takes the form of emails sent by a company's information technology team simulating common phishing attack strategies to determine whether employees can identify and distinguish legitimate emails from phishing scams, and whether they will report the latter to their company's information security team.

Falling for a phishing test email once or twice is usually not a critical issue for a company (and may even incentivize an employee to be more vigilant upon being made aware of their susceptibility). Repeated failures, however, may spur a company to consider implementing some remedial measures to ensure that such employees do not fall prey to a real phishing attack because of the known risk that phishing test failures can present. For example, in the event that a company experiences a major cybersecurity incident, if the root cause was a successful phishing attack on an individual that was known to have failed consecutive phishing tests without sufficient (or any) corrective actions taken, that company may have difficult questions to answer from regulators or plaintiffs' lawyers. But remedial measures present their own risks and challenges.

Remediation Challenges

- **Failing Employees May Be Hard to Discipline.** Some of the employees who are most likely to fail phishing tests are senior executives, who often receive hundreds of emails a day, while multitasking several personal and work-related issues simultaneously, and may be specifically targeted (i.*e.,* spear phished) because of their access to sensitive information. These employees may also be the least likely to prioritize the time to participate in phishing training and testing in the first place, and companies may be reluctant to subject senior individuals to supplemental phishing training or discipline.
- **Employment Law Issues.** Any remedial measures that could be considered as a disciplinary sanction must take into account the employment law requirements of the relevant jurisdiction. In the United States, employers generally have leeway when determining how to discipline at-will, non-unionized employees. In the United Kingdom, however, employees generally need to be warned in advance that failing to comply with the employer's cybersecurity measures may have disciplinary consequences up to and including termination of employment. In other European jurisdictions, introducing sanctions may also require prior engagement with employee representatives. In most jurisdictions, any employment agreements and the requirements of labor codes would need to be assessed to determine whether failure to pass phishing tests, or falling victim to genuine phishing attempts, would

fall within the circumstances permitting significant discipline or termination without notice.

- **Creating the Right Cybersecurity Incentives.** Severe discipline for failing phishing tests may create the wrong incentives for employees who may be reluctant to report when they think they have fallen victim to a phishing attack for fear of being fired, thereby making the company less secure.

Considerations for Dealing with Phishing Failures

In light of these challenges, there is no single correct approach for phishing failure remediation. In crafting a corrective-measures policy, employers should consider the following:

- **Fair Testing**. Companies should try to ensure that their phishing tests match the level of sophistication of the phishing threats that the tested group of employees face, and not be so difficult that employees who would likely detect a real phishing email would be fooled by the test.
- **Consistent Application of Remedies**. Companies should try to ensure that the remedies they employ are consistently applied throughout their business (*i.e.,* not just to low-level employees, where risk may in any event be limited).
- **Remedial Training and "Tone from the Top"**. For employees who repeatedly fail phishing tests, companies should consider requiring remedial training, as well as messaging from senior executives as to the importance of phishing training and testing to the overall goals of the organization.
- **Name and Shame**. Companies may consider "name and shame" tactics, whereby the names of individuals who fail phishing tests are publicized in an attempt to create incentives to take the training and testing more seriously. Such tactics, however, can harm employee morale and create friction with information security personnel.
- **Stricter Controls**. Companies can implement additional technical controls to reduce the chances of phishing attempts reaching certain end users who are deemed to be at high risk of clicking on phishing emails. These measures can include having an IT professional pre-screen all emails with links and attachments before they reach the end user. While such measures may be effective, the associated resources may limit their practicality and scalability.
- **Disciplinary Measures**. In certain circumstances, employee disciplinary measures may be appropriate. Just as employees may reasonably expect consequences if they fail to comply with company-mandated physical security measures (*e.g.*, knowingly allowing third parties to access company premises without authorization or negligently leaving hard copy confidential information in public), employees should expect consequences for failing to follow reasonable cybersecurity precautions. But care must be given to ensure that the discipline is properly tailored to the risk and doesn't result in unintended consequences, for example, a significant reduction in productivity due to employees unnecessarily reviewing every email very carefully.

One possible disciplinary measure is denying email access to employees until they complete certain remedial training and score sufficiently well in a phishing test. Whether this is an appropriate measure will obviously depend in part on the individual's role in the company and the possible associated business disruption.

Phishing testing is an important aspect of most companies' cybersecurity programs, but to get the full benefit of that testing, and to avoid unnecessary problems, companies should carefully consider what measures, if any, should be implemented for employees who repeatedly fail those tests.

"To subscribe to the Data Blog, please click here."

Avi Gesser

Avi Gesser is Co-Chair of the Debevoise Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy and artificial intelligence matters. He can be reached at agesser@debevoise.com.

Jeremy Feigelson

Jeremy Feigelson is a Debevoise litigation partner, Co-Chair of the firm's Data Strategy & Security practice, and a member of the firm's Intellectual Property and Media Group. He frequently represents clients in litigations and government investigations that involve the Internet and new technologies. His practice includes litigation and counseling on cybersecurity, data privacy, trademark, right of publicity, false advertising, copyright, and defamation matters. He can be reached at jfeigelson@debevoise.com.

Tricia Sherno

Tricia Bozyk Sherno is a member of the Debevoise Litigation Department, concentrating in employment and general commercial litigation. She has a broad-gauged employment law practice, with experience representing clients in matters involving discrimination and harassment, contracts, corporate raiding and compensation

across a broad range of industries. Tricia can be reached at tbsherno@debevoise.com.

Christopher Garrett

Christopher Garrett is an English-qualified international counsel in the Corporate Department and a member of the Data Strategy & Security practice, practising employment law and data protection. He has significant experience advising employers on all aspects of employment law and advising companies on compliance with UK and EU data protection law. Mr. Garrett has substantial experience in advising on the employment aspects of mergers & acquisitions transactions, including transfers of employees or other issues arising under TUPE/the Acquired Rights Directive. Mr. Garrett has a wide range of experience advising on other matters such as boardroom disputes, senior executive contracts and terminations, disciplinary and grievance matters, a variety of employment tribunal claims (including high-value discrimination claims), advising employers faced with industrial action, consultation on changes to occupational pension schemes and policy and handbook reviews. Mr. Garrett also has a particular focus on handling privacy and data protection issues relating to employees, as well as online privacy, marketing and safety practices, regular advice to clients on privacy policies, online marketing practices and related matters.

Stephanie Cipolla

Stephanie Cipolla is an associate in Debevoise's Litigation Department who is a member of the Debevoise Data Strategy & Security practice. She can be reached at smcipolla@debevoise.com.

Jose Angel Lamarque III

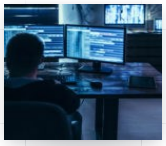
Jose Angel Lamarque III is a corporate associate and a member of the Debevoise Intellectual Property and Mergers & Acquisition Groups. He is also active in the Debevoise Data Strategy & Security practice. He can be reached at jalamarque@debevoise.com.

PREV POST

Preparing for and Responding to Ransomware Attacks: Thirteen Lessons from the NIST Framework and Recent Events

NEXT POST

Business Email Compromise: Who Bears the Loss?



Related Posts

Four Takeaways from the SEC's Proposed Cybersecurity Rules

FEBRUARY 16, 2022

Webcast – Fireside Chat with NYDFS Cyber Chief Justin Herring

FEBRUARY 5, 2022

Credential Stuffing Continues Practical Guidance to Protect Customer Information

JANUARY 31, 2022