Keeping Your Organization Secure During the Coronavirus Pandemic

As Coronavirus continues its spread across the globe, the world has changed faster than most of us ever imagined it could. Organizations big and small are facing new realities, as they work to keep employees safe and serve customers and partners to the best of their abilities.

Unfortunately, there are those who view this crisis as an opportunity, and they are proactively looking to exploit it. Cyberattacks targeting end-users are the easiest way to take advantage of employees unaccustomed to working from home and stakeholders of all types who are simply looking for information and guidance.

At Mimecast, we are seeing this scenario play out both across our global customer grid, where malicious email-based attacks have increased dramatically, and on the web, where fake websites are being spun up at an alarming rate. We are committed to helping our employees, customers, partners, and the larger cybersecurity community successfully navigate these uncharted waters.

The guide that follows is intended to provide IT and security teams with practical, actionable advice on how to help reduce risk and remain resilient during this unprecedented public health crisis. In addition, you can live chat with Mimecast's cybersecurity experts and get information about how to manage rapidly changing security and data protection requirements by visiting our **Coronavirus Response Page**.

Security for Remote Employees

The most immediate challenge most IT and security teams are facing is ensuring employees can work securely from home. The following are some steps you can take to help reduce risk. **Click here** for a model of a standard communication you can send to employees to increase their awareness, as well as a **training video** to help reinforce the concepts.

1. **Secure Web-Based Activity –** Without the protection of a network firewall and often limited endpoint web controls, the likelihood of web-based attacks succeeding goes up dramatically. Applying protection with a cloud-based web security service that includes an agent on all devices allows you to block malicious web-based content, while also enforcing acceptable use policies and tracking activity, regardless of where the user is physically located. Security checks happen seamlessly, in real-time, and in the background, so end-users can work securely from various types of devices with no impact on productivity. To help organizations address the web security challenge, we are providing all Mimecast customers with access to our web security service at no cost for 90 days. **Click here** for details and terms and conditions.

2. **Ask Employees to Update Contact Information –** IT and security teams will need valid mobile phone numbers to confirm employees' identities for activities like resetting passwords, notifying them if a security breach occurs, approving quarantined devices when adding email to mobile phones, and of course, contacting them in case of emergency. This is a great time to encourage all employees to update their information.

3. **Simplify Activities that Lead to Policy Violations –** The use of unsanctioned applications is likely to increase during this work from home period; so simplifying and speeding tasks, such as sending large files or sensitive data, with technology that integrates directly into the corporate email system can significantly increase adherence to organizational standards. Policies like data loss prevention can also be automatically triggered. In addition, monitoring the use of unsanctioned apps can help you assess risk on an on-going basis and proactively address violations as needed.

4. **Continuously Raise Awareness About Cybersecurity Risks –** Simply letting employees know about the increased risk and providing guidance about what to watch out for can go a long way toward helping mitigate risk. Mimecast will be providing updates on emerging attack types through our **Coronavirus Response Page** and regularly scheduled informational webinars, so you can stay informed and update your end-users as needed.

5. **Review your authentication processes to ensure they're adequate in a work from home situation.**

Operational Continuity and Data Protection

As email attack volumes grow in the wake of the pandemic, the likelihood of data being exposed or business services being disrupted goes up as well. The following steps can help you remain operational when disruptions occur, while also ensuring data is not lost.

1. **Institute an Email Continuity Plan –** Email is a critical communications channel at the best of times, and current conditions make insulating your organization against an outage even more critical. Continuity technologies can route your email through a cloud-based service, whether email is on-premises, in the cloud, or a combination, and give end-users uninterrupted access to live and archive email using the tools they already know. Continuity can be activated by administrators, who can be notified of issues and kept informed through various types of alerts.

2. **Review and Reinforce Data Recovery Capabilities –** Many organizations have data recovery gaps that they are not aware of until they need to recover lost or stolen information. These gaps are often related to end-user restoration limits, the need for multiple retention policies that conflict, and the lack of native backup. Now is a good time to review your capabilities and ensure you can easily provide granular, point-in-time recovery of emails, files, and contact data for all users.

Brand Protection

Brand exploitation is extremely common in times of crisis, with criminals using a variety of tactics designed to trick unsuspecting and vulnerable people. These brand-based attacks can be difficult to detect and remediate, but there are some steps you can take to protect employees, customers and, partners, as well as your organization's reputation.

1. **Review and/or Implement DMARC Policies –** Attackers will often use your legitimate domains to send fake emails that are incredibly hard to detect. DMARC is an email authentication protocol that can help you prevent and shutdown this activity by controlling who's able to send email using domains your organization owns, whether active or dormant. DMARC policies can also help you block inbound attacks by setting policies that instruct ISPs to delete or deliver emails. For more information, visit **https://www.dmarcanalyzer.com/dmarc**.

2. **Monitor the Web for Lookalike Websites –** It is easy for cyber criminals to register fake domains and create websites that look like yours with the intention of spreading disinformation and tricking unsuspecting visitors into divulging sensitive data through phishing and other malware campaigns. These attacks are particularly dangerous and damaging in our current situation. Security technology can be used to scan the web for these attacks and either detect them in their early stages or have live sites quickly taken down.

Coronavirus has resulted in an unprecedented level of global disruption, and the situation is evolving rapidly. Mimecast is committed to helping you stay informed about changes in the cybersecurity threat landscape and strategies you can use to help keep your organization as secure as possible.

Please reach out via the live chat feature on our **Coronavirus Response Page** with any questions you may have or ideas you'd like to share with our larger community. Our hearts go out to everyone who has been affected by the COVID-19 virus in any way, and we wish all our customers and partners the very best in this difficult time.

Mimecast's Guidance to Our Employees

Like many organizations, Mimecast has closed its offices and implemented a work from home policy until further notice. The following are some reminders we are sending our own employees:

- Secure your home Wi-Fi with a strong password that is at least 10 characters long and uses a combination of upper and lower-case letters, numbers, and special characters.
- Update your personal contact information in our system.
- Don't click on any links or attachments related to COVID-19 that are received from outside the organization via email or messaging apps, including personal email providers like Gmail.
- Pay close attention to messages that appear to be from a trusted source, like the World Health Organization (WHO) and U.S. Center for Disease Control and Prevention (CDC), and closely inspect the sender's email address and any URLs in the message.
- Report anything suspicious, such as emails, links, phone calls, and instant messages.
- Don't click on links in emails that ask you to enter or update your username and password. Type URLs directly into a browser, rather than using links, and be 100% certain you are on the correct site before logging in.
- Don't install any applications that haven't been approved by IT and Security, as these can have vulnerabilities.
- Don't disable any security features, such as firewall settings, web security settings, and antivirus settings, on your devices.
- Always follow our Acceptable Use Policy, especially around personal use of laptops and other IT resources.