mimecast®

The Year of Social Distancing

Security Challenges of the New Digital Workplace

March 2021

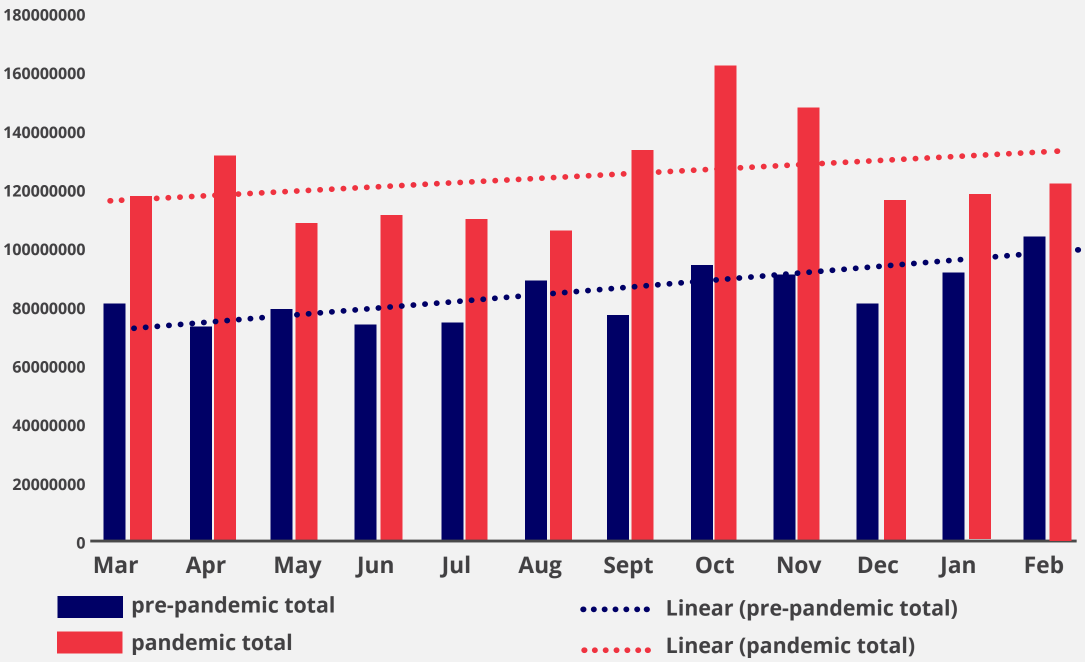
There have been events throughout history that have caused a fundamental transformation of society on a global scale. The harnessing of electricity, the internal combustion engine, the two world wars and the internet come to mind. However, none of these caused a global transformation of society as quickly as did the COVID-19 pandemic.

COVID-19 was first reported on New Year's Eve 2019 and was declared a pandemic by the World Health Organization in March 2020, causing much of the world to implement social distancing guidelines and other protective measures, including lockdowns. Arenas, train stations, office buildings and other venues that normally attract bustling crowds were empty, as people retreated to their homes to protect themselves and their loved ones from the pandemic.

In the year since lockdowns began, there has been an explosion of innovation and digital transformation as organizations transitioned to fully remote work and digitized business processes. The slowly evolving digital workplace of 2019 had fully arrived by mid-2020. (The running joke became "we started the year in 2020 and ended it in 2030.")

As with every major, chaotic event, threat actors immediately took advantage of the uncertainty and worry around the world. The mass anxiety around the COVID-19 pandemic created an opportunity-rich environment for social engineering attacks. In fact, Mimecast detected an average 48% monthly increase in threat volume in The Year of Social Distancing when compared to the previous year.

Mimecast Detection Camparator: Pre and Post Pandemic



48%

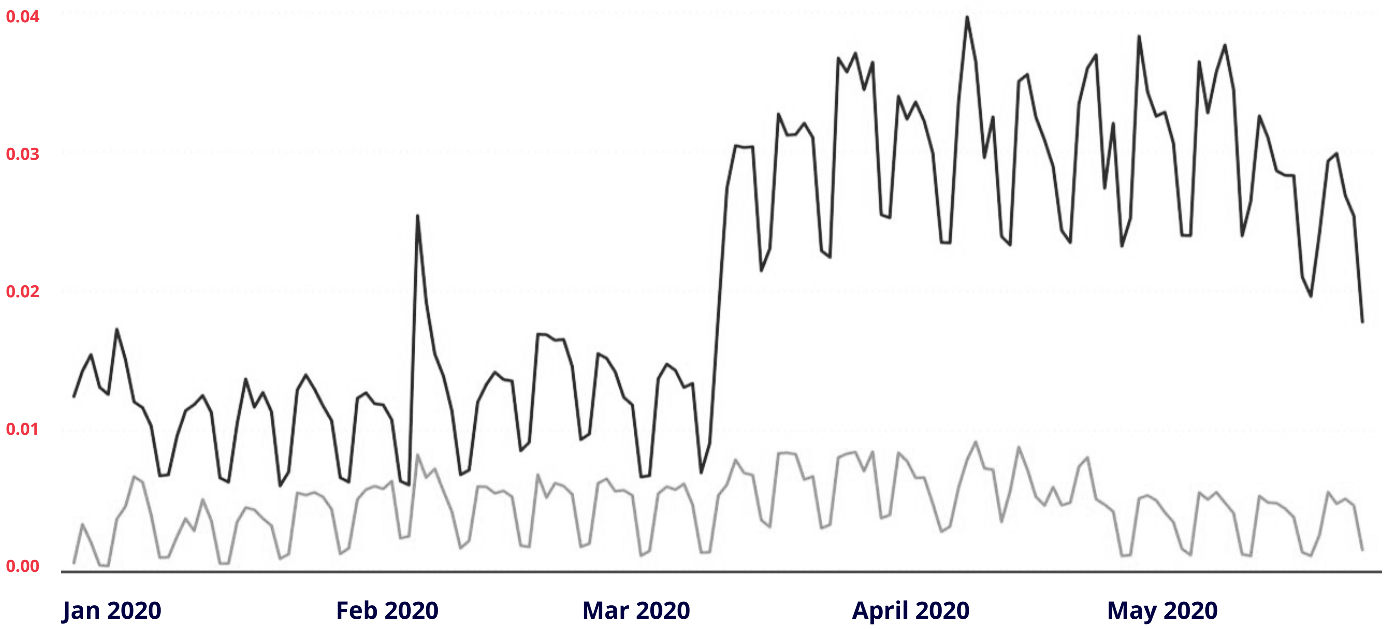
Mimecast found a 48% increase in threat volume in March 2020 – February 2021 over the previous year, and the increase coincided with the onset of the COVID-19 pandemic.

The digital workplace under attack

With employees moving into the work-from-home model, the digital workplace became a reality for organizations worldwide. Cubes, offices and conference rooms were replaced by email, instant messaging and Zoom meetings. Many organizations were able to continue operations this way with only minimal disruption – however, cyber risk escalated considerably. For one thing, out of necessity, there was an increase in the digital transfer of sensitive content. Topics that previously would have been discussed in conference rooms or sketched out on white boards were now being discussed over collaboration tools and shared over email.

A key escalator to cyber risk, however, is employee behavior in the home. People simply are not as vigilant about cybersecurity when they are home, as was evidenced by Mimecast finding a 3X increase in unsafe clicks (clicks on malicious URLs in emails) by employees worldwide during the time when social distancing and lockdowns were going into effect.

Average Number of Unsafe Clicks Per User



3x

There was a 3X increase in unsafe clicks when work-from-home began.

Mimecast research from September 2020 also found that cyber hygiene habits vary from country to country. For example, U.K. and German workers are about half as likely to open suspicious emails compared to U.S. workers.

34% **Brits & Germans opening suspicious emails**

60% **Americans opening suspicious emails**

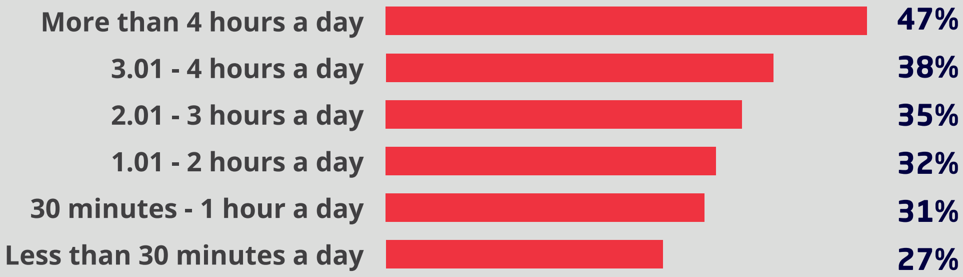
61% **Emiratis opening suspicious emails**

Americans and Emiratis are nearly twice as likely to open suspicious email than workers in the United Kingdom and Germany.

60% ⇧

Employees surveyed in Mimecast's research also indicated a **60% increase in the use of company-issued computers for personal business** since the beginning of the COVID-19 pandemic.

Personal use of corporate devices per day



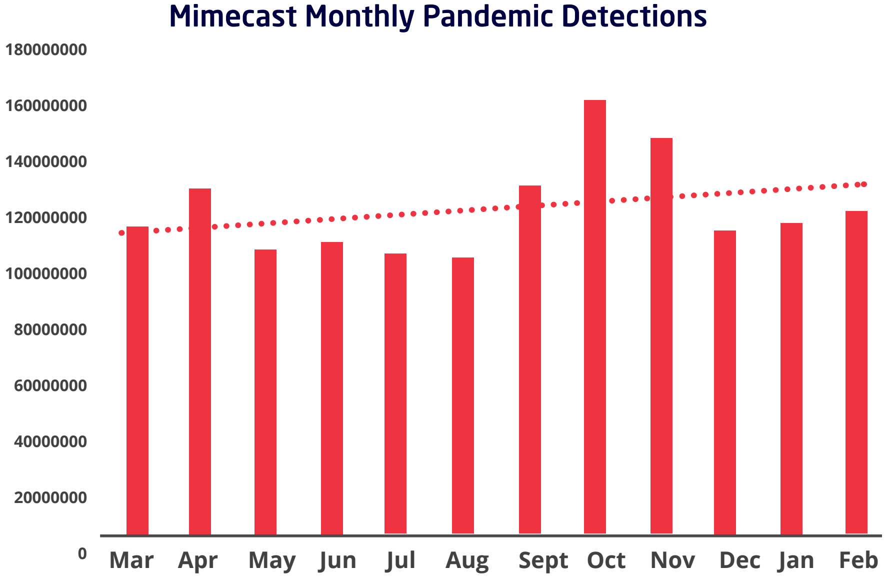
Personal use of company-issued computers has risen dramatically during the pandemic.

Threat actor tactics

Threat actors use crises as an opportunity to launch social engineering attacks. We see this any time there is a natural disaster or some other event that causes people to become distracted, stressed and more likely to be deceived by social engineering attacks.

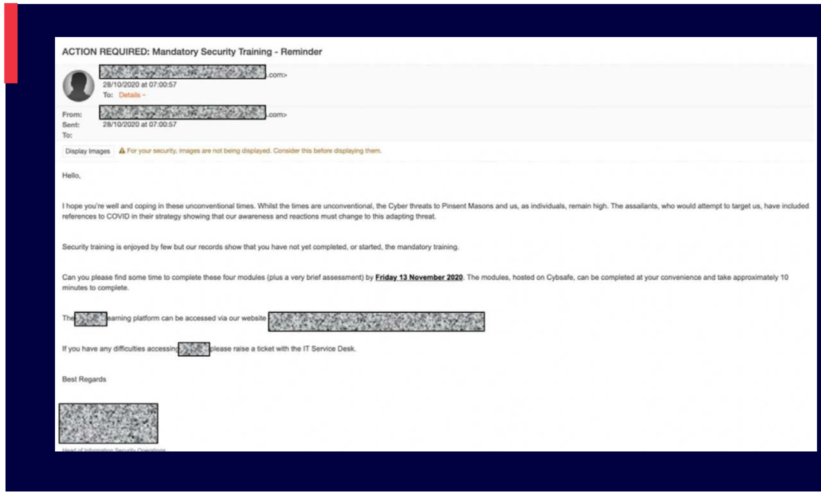
However, while most disasters are regional in nature, and thus only applicable to a subset of people in a particular country or region, the COVID-19 pandemic has provided a perfect storm to threat actors since it is a disaster that impacts the entire world.

Threat actors have capitalized on the global human misery. Overall threat volume grew 48% year over year. The figure below shows how threat volume spikes in April and October coincide with the COVID-19 infection peaks during 2020.



As mentioned earlier, part of the motivation for this dramatic increase in attacks is to "flood the zone" with alerts in SOCs, to increase the likelihood that inundated security analysts will miss identifying attacks.

COVID-related phishing attacks took many forms. Some sought to make recipients sympathetic to the sender's plight and defraud them of money; others purported to have important COVID-related information for the recipient. For employers, the most concerning were those designed to steal worker credentials. The email below is one such attack, attempting to trick employees into responding to a "mandatory security training" online course.



ACTION REQUIRED: Mandatory Security Training - Reminder

[redacted].com>
28/10/2020 at 07:00:57
To: Details ~

From: [redacted].com>
Sent: 28/10/2020 at 07:00:57
To:

Display Images
⚠ For your security, images are not being displayed. Consider this before displaying them.

Hello,

I hope you're well and coping in these unconventional times. Whilst the times are unconventional, the Cyber threats to Pinsent Masons and us, as individuals, remain high. The assailants, who would attempt to target us, have included references to COVID in their strategy showing that our awareness and reactions must change to this adapting threat.

Security training is enjoyed by few but our records show that you have not yet completed, or started, the mandatory training.

Can you please find some time to complete these four modules (plus a very brief assessment) by **Friday 13 November 2020**. The modules, hosted on Cybsafe, can be completed at your convenience and take approximately 10 minutes to complete.

The [redacted]earning platform can be accessed via our website [redacted]

If you have any difficulties accessing [redacted] please raise a ticket with the IT Service Desk.

Best Regards

[redacted]

Head of Information Security Operations

As seen in the email example above, threat actors sought to exploit the trust of the employer/employee relationship to steal credentials and gain access to employer networks and systems.

This type of tactic is just one way that threat actors seek to use home networks as a conduit to compromise workers, allowing them to gain unauthorized access to corporate networks and systems.

While the COVID-19 pandemic was a dominant theme for social engineering attacks in The Year of Social Distancing, it was not the only one. There were a number of additional significant themes and developments during the year, including:

Attacks on the healthcare sector. Another way threat actors took advantage of the COVID-19 crisis was to launch attacks on overstretched healthcare systems. Both the U.K.'s National Cyber Security Center (NCSC) and the U.S.'s Federal Bureau of Investigation (FBI) issued warnings to the healthcare sector in May 2020. Threat actors sought to exploit increased human error associated with the stressful conditions to steal data and infect systems with ransomware-based attacks, under the belief that organizations operating under urgent conditions are more likely to pay ransoms – in this case, hospitals urgently trying to protect the health of their patients.

Attacks on vaccine developers. In July, the NCSC and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued a joint warning to vaccine developers about nation-state attacks. These attacks were aimed at stealing intellectual property and undermining the U.S. response to the COVID-19 crisis.

Attacks on schools. With schools urgently working to reopen in some fashion as fall approached, threat actors launched ransomware attacks, realizing schools are often poorly defended, facing a deadline to begin instruction, and sitting atop operational budgets that could be tapped for ransom.

The summer of ransomware. Mimecast reported the return of Emotet to the threat landscape in July 2020, after a five-month hiatus. This malware dropper is frequently used to deploy the Trickbot trojan as a second-stage infection, which can then be used to infect machines with ransomware. Mimecast detected increasing volumes of ransomware throughout the summer (although not all can be attributed to Emotet).

Attacks on the vaccine supply chain. As 2020 drew to a close and vaccine rollouts began, Mimecast predicted with a high degree of probability (80% - 90%) that threat actors would begin targeting companies in the vaccine supply chain. Once again, they will target companies in a state of urgency because they are more vulnerable to payment demands.

Lessons learned from The Year of Social Distancing: Cyber deception is the problem

Mimecast has assessed the likelihood of threat actors continuing to exploit the unsettled work situation as almost certain (95%). These efforts will focus both on remote workers and those returning to the office, which creates a whole new range of social engineering opportunities. Threat actors always exploit turmoil – whether that turmoil is brought on by unexpected natural disasters, annual events such as tax season, or a once-in-a-century pandemic. So if we know this, why do they continue to be successful?

The answer lies in the compartmentalized way in which companies think about security. **While security organizations think in terms of email security, user awareness, link scanning, identity management, and so on, threat actors are thinking in terms of deception campaigns.** Just like a magician uses multiple tools (misdirection, lights, special props, etc.) to deceive the audience into thinking that one thing is happening, only to have another thing happen, threat actors do the same thing using multiple orchestrated tactics and tools to deceive people into drawing the wrong conclusions, so they are free to execute their attacks.

And, just like magicians would be ineffective if the audience had complete visibility into their activities, the best way to defeat threat actor cyber deception is to gain greater visibility into their campaigns. Defense-in-depth remains an important foundation of security strategy; however, it has also contributed to the infrastructure bloat issue that plagues many companies – too many security tools, too few people to manage them all.

Part of the solution to this problem is integration: by integrating best-of-breed cyber security tools, organizations can gain much greater and more precise visibility into cyber deception campaigns to stop them earlier in their development.

These cyber deception campaigns include three components: preparation, execution and exploitation. Too often, security strategy is singularly focused on exploitation. Even the incident detection and response process inherently means an incident has happened, and the company is in reactive mode minimizing the damage.

By adopting an integrated counter-deception strategy, companies can disrupt campaigns before they reach exploitation through proactive measures during the first two stages of the campaign:

Preparation Stage

Threat actors conduct their own reconnaissance, researching employees and companies on social media to improve social engineering attack effectiveness. They also might spoof trusted domains – such as the employer's website, or the employee's personal bank - in preparation for the execution stage.

Protection: An effective counter-deception strategy and supporting tools will identify these activities early in the campaign cycle and apply countermeasures.

Execution Stage

While one-off attacks are likely to remain a tool in the threat actor's arsenal, the most damaging attacks usually require more patience and planning. Sophisticated threat actors will use multi-vector sequences that include elements like elaborate chains of communication with the victim to establish trust, the use of look-alike domains, fake LinkedIn profiles, and scraped web pages. All of this is designed to meaningfully add to the impression of authenticity.

Protection: A combination of end-user cyber security awareness training and good internal processes, combined with technology that can help identify suspicious behavior, can help disrupt this execution phase before major damage is done. For example, warning the accounts payable department that a payment request has originated from someone who appears to be making fraudulent use of a logo can prevent business email compromise from being successful.

Like other major historical events, the Year of Social Distancing shed light on weaknesses in organizational resilience models. With cybersecurity, we saw the deficiency in pre-existing compartmentalized security strategies. By evolving security strategy to a model designed and implemented to counter deception, organizations can uncover deception campaigns earlier in their development cycle, and have built-in programs that help prevent disturbing developments like the 3X spike in bad clicks that Mimecast observed in March 2020 when work-from-home became the norm for much of the world. And, when the program is built in this way, it is much more resilient in the face of massively disruptive events – even a once-in-a-century pandemic.

mimecast®

Relentless protection. Resilient world.™