

Mimecast: how COVID-19 highlighted the value of security awareness training

Mimecast

Phishing

Security

4th June 2021



Below, Mimecast explains why effective security awareness training has become more vital than ever.

As work moved from the physical to the virtual to allow for social distancing during the COVID-19 pandemic, the need for cybersecurity increased. Confidential in-person meetings have been replaced with videoconferences using software that may not be secure, and employees have been accessing company networks from outside the office. With more targets for cyberthreats, effective security awareness training has become more vital than ever.

Employees working virtually need extra security awareness training

In order to safeguard data when employees do more work online, companies should address some of the most common cyber threats.

Phishing increases when companies rely more on email

Cyberthieves often steal sensitive information with phishing attacks. Phishing emails appear to be from a trusted sender, and they trick people into revealing sensitive information. As virtual work increases the need for email communications, opportunities for phishing increase.

Security awareness training teaches employees to recognize the signs of phishing, including:

- An email address that doesn't come from a real company domain name
- Misspelled words or poorly worded phrases
- Requests to enter passwords or sensitive information in a pop-up window

Employees working from home can't call over a co-worker for a quick opinion on a suspicious email. Without the ability to get an immediate second opinion, an employee is more likely to click on a malicious link.



Trending

How order management software transforms your business

Data created at home is more susceptible to hacking or data leaks

Employees need training in how to keep their home offices as secure as the company's office. The following techniques should be covered in security awareness training:

- Making sure all company data is encrypted
- Using only secured Wi-Fi networks
- Using passcodes on mobile devices
- Protecting data from unauthorized users in the home

Employees using personal devices may be more susceptible to ransomware

Ransomware is software that an attacker loads onto a computer to encrypt the data. The software installs on a computer when someone clicks on a link in the attacker's email and then can't access their data until they pay a ransom to the attacker.

If companies allow employees to use personal devices, they should require the use of anti-virus and anti-malware software. Employees should also be sure to back up company data regularly so they can access the backup and avoid needing to pay a ransom in the worst-case scenario.

READ MORE:

- [Inside Mimecast's The State Of Brand Protection 2021](#)
- [ServiceNow delivers new security integrations with Microsoft](#)
- [Microsoft and Darktrace join forces to provide self-learning AI cybersecurity to users](#)
- [What can corporates learn from digital transformation in the COVID era?](#)

Strategies for security awareness professionals

Some considerations for setting up a security awareness training program include:

- Identifying the security risks the company's employees will likely face. Examples include hacking, phishing and ransomware.
- Identify the organization's legal responsibilities for protecting data. The privacy act of 1974, HIPAA, and the Gramm-Leach Bliley Act (GLBA) are just some of the regulations that govern data handling.
- Evaluating the best way to deliver security awareness content. Will employees watch a video, or will a more interactive strategy be more effective? Using a research-based, professionally developed security awareness training, rather than attempting to develop one in-house, can help improve efficacy.
- Assess who should be in the target group. Some employees may not have access to sensitive data, so security awareness training is less necessary for them.

For more news from Top Business Tech, don't forget to subscribe to our daily bulletin!

Follow us on [LinkedIn](#) and [Twitter](#)

