mimecast

3 Ways AI Is Changing Email Security for M365 Admins... and 3 Ways It's Not

Artificial intelligence (AI) is a great contributor and potential threat. When it comes to email security, AI is being used both by bad actors and organizations looking to prevent cyberattacks. But just because AI is a relatively new tool, it doesn't mean that everything is changing. Here are three ways AI is changing email security and three ways it's staying the same.

What's New

Phishing at Scale

Phishing is a bad actor favorite. It's cheap to execute and is a direct path to an organization's employees. AI can be used to **launch customized phishing campaigns using GPT.**

More Well Researched Content

Social media and LinkedIn made it much easier to create well-researched phishing emails. AI tools make it even easier. With a few simple AI queries, content can be generated that appears to be written by someone familiar with you or your company.

Greater Potential for Coordinated Attacks

While most attacks only use email to target employees, AI-based tools are making it easier to combine multiple channels to **increase the believability** of an attack, e.g., attacks that combine email with phone, or email with collaboration tools, could be even more convincing for employees to take the action the attacker wants.

What's the Same

Same Attack Types

Whether or not they use AI, email attacks require a malicious payload or some type of impersonation attack to either steal credentials, money, other value, or information. **Cyberattacks** must have a monetization or disruption benefit to attackers.

Be Wary of Unexpected Emails

Getting an email from someone you've never corresponded with or from a domain you've never seen can be an obvious phishing clue. With AI tools, suspicious emails are more likely to come from known colleagues and trusted domains. Users need to be even more wary of unexpected emails, especially emails asking for information or to initiate monetary transactions.

Speed of Response Is Everything

The quicker an organization can respond to an email-based threat, the better. In the case of AI-generated email, it's important to ensure that security policies are in place to quarantine suspicious emails and to have remediation steps for a SOC team to take.

AI is already changing the email threat landscape. Knowing the risks will better equip your organization to take the steps necessary to limit the threat of cyberattacks. To learn more about how Mimecast can help M365 admins with email security, visit **mimecast.com/work-protected**.