Keeping Phishers at Bay with AI

In this area, machines just might be able to do better than humans.

Kevin McCaney

Mon, 04/02/2018 - 09:25

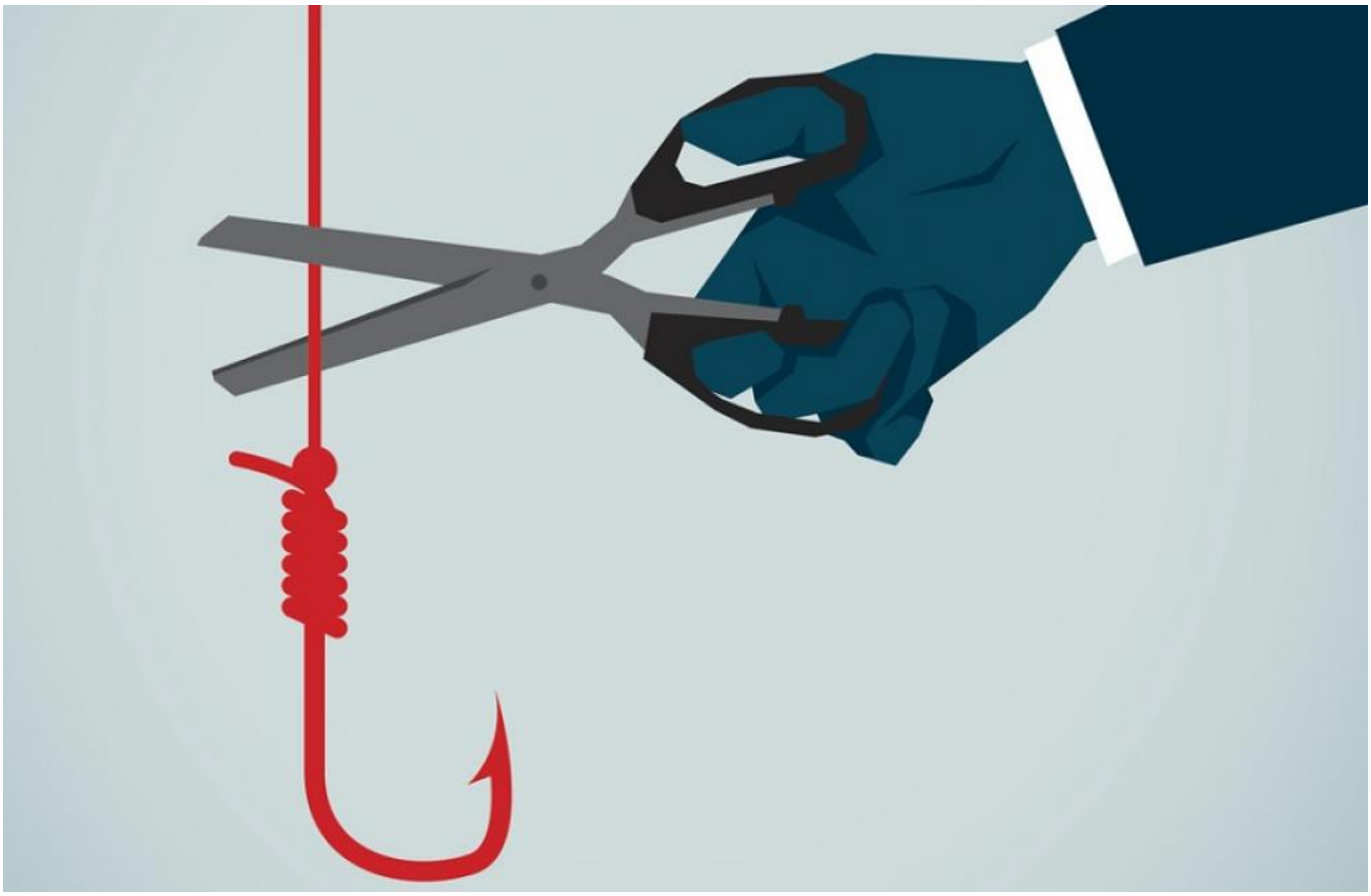

Illustration: erhui1979/iStock

For all of the sophistication involved in online espionage, thievery and disruption, the first step usually is a simple one: hoodwinking people with tactics at least as old as the Victorian-era swindles started with hand-written letters. Phishing campaigns today most often come via email, apparently from a trusted source, with a message designed to fool the recipient into clicking a link and/or giving up their passwords to targeted systems.

William Evanina, director of the Office of the Director of National Intelligence's National Counterintelligence and Security Center, recently said 90 percent of successful data hacks of government and industry in recent years started with

spear-phishing attacks — phishing campaigns targeting specific people, as opposed to the mass mailings favored by Nigerian colonels.

Any number of cybersecurity studies, along with the most high-profile attacks in recent years, back up that assertion. Phishing was the foot in the door in large-scale data breaches involving Google, Sony and Target, for instance, and was likely the first salvo in the hack of the Office of Personnel Management, which exposed personal information on more than 20 million people who had undergone background checks, including current and former federal employees, family members and contractors (and which was followed by a separate phishing campaign masquerading as official notifications about the hack).

Taking Humans out of the Equation

The weak link in these scenarios are users, who despite awareness of the problem can still miss some of the clues an email or website is spoofed and wind up making a fateful click. A recent study by Glasswall Solutions found 82 percent of employees who'd had email security training will open email attachments if they appear to come from a known source, and almost half of those will click every link they get.

Phishing works because social engineering works, and social engineering works because people are human. Whether they're busy, distracted or just inattentive, they can be tricked. In this area, machines just might be able to do better.

Anti-phishing programs have been a part of organizations' cyber defenses for a while, but as phishing and other attacks become more crafty — aided, not coincidentally, by machine learning and artificial intelligence — AI could help improve their effectiveness.

AI's ability to quickly analyze data, spot anomalous patterns and learn from past examples can help against spear-phishing tactics. Those tactics can vary in content from phone messages posing as legitimate business matters, to billing "emergencies," investment opportunities, lottery scams, and notices from government agencies. What they often have in common is the use of spoofed email addresses and websites.

The federal government is trying to tackle these spoofing tactics with DMARC, the Domain-based Message Authentication, Reporting, and Conformance specification

designed to prevent domain spoofing by requiring additional authentication techniques.

Not Taking the Bait

DMARC is an email authentication, policy and reporting protocol that OKs emails from legitimate domains and rejects those that are not. As the National Institute of Standards and Technology explains in a publication on trustworthy email, DMARC "was conceived to allow email senders to specify policy on how their mail should be handled, the types of reports that receivers can send back, and the frequency those reports should be sent."

It doesn't defend against all of the tactics used in phishing, but it does prevent spoofing. It won't be fooled, for example, into thinking that amazonn.com is amazon.com, or that a link to bankofamerica.login-now.info is actually going to bankofamerica.com.

The Homeland Security Department has mandated federal agencies employ DMARC, but full adoption has run into a couple hurdles. About half of agencies failed to meet a Jan. 15 deadline for deployment, and although a DHS spokesperson told CyberScoop this month over two-thirds had adopted DMARC, some agencies may have misconfigured it, failing to account for spoofed subdomains and leaving themselves open to attack.

Configuration is a challenge with DMARC, because of complicated formatting and other issues, as well as the fact that organizations do business with a lot of legitimate entities, so there is a lot to keep track of. Advanced analytics and AI can streamline configurations and management. Barracuda offers one approach with its Sentinel product, a cloud service that works with the DMARC specification, with a wizard-based configuration process and AI-enabled pattern detection that searches for anomalous behavior. Another example is Vade Secure, which uses AI and behavioral analysis to detect the subtle signs of a fraudulent email, even in one-off attacks.

That's just one area where AI can help. AI and machine learning systems can — and already are — be used internally to monitor networks for signs of malicious code or unusual actions by insiders. Those programs focus on what's gotten inside a network. By applying AI to email monitoring and anti-phishing practices, organizations could stop at least some of those attacks at the gate, before they can

get in, and sometimes before they can even knock on the door.

View printer friendly version
Artificial Intelligence
AI
Federal Cybersecurity
phishing
social engineering
Duplicate
Eye on AI