Science Translations
Established 1990
PC410.COM™
PC Updater News

AI is Building Smarter Phish

Security software has gotten pretty good at identifying bad files nowadays. And proper security steps, like never using Administrator credentials to do work, will block nearly all the attacks that Microsoft is constantly patching. So that's three layers of protection. Add to that automated patching of third-party programs, email spam filters, and what's left to fix? Well, common sense seems to be the last install needed in some offices. That's right, humans have to recognize bad emails and AI fakes of voicemails from their boss.

However, AI is making all these threats less obviously fake. Given a sample of your email, or email from someone who regularly exchanges emails with you, it's possible to create a very convincing email that asks you to open an online 'document' that is really a password stealer. Until now, these were very generic bulk attacks. The hackers just send out a few million emails with an urgent message to open a document right this instant because, well, because they say so, and a tiny fraction of the recipients followed those instructions and lost control of their computers, emails, and bank accounts. So what changes when cheap AI enters the mix?

Hack scenario: One of your email correspondents has had their email password compromised. Because their entire email file is online (using IMAP or MS365/Exchange mail), many years of emails become AI training documents. Then that AI can spear-phish (micro-target) the correspondents found in that email treasure box. The result is a very believable set of payment instructions, or a 'read this document on Google Drive' instruction.

Prevention: Your staff has to know that starting a new payment method based only on an email or a voicemail from (apparently) their boss or customer is not allowed. And that payments cannot arrive in an attachment or an online document. And that the IRS will never ask for payments by email or by phone.

They also need to understand phish, spear phish, and some more terminology:

Phish: It's bait, like what would be used in fishing, but you're the catch. These are mostly emails, with a false-urgency message to click through to a document, attached or maybe online, and they claim to be very time-limited. Some of these lead to malware and ransomware, but many lead to fake login screens that will capture logins and passwords for mail accounts and banks.

False Urgency Syndrome: Dangerous messages are frequently made to look important, very timely, and scary to ignore. These are common scam messages that use false urgency:

- An account is full. Click to fix now. (It's an attempt to capture email logins.)
- A very large purchase order has arrived. Grab the document from our Google Drive account, or Docusign, a fax service, or any legit file sharing service. (That is trying to deliver malware, basically a trojan horse.)
- We're filling your unrealistic and expensive order today for a dozen iPads. OK? (They want a cancellation phone call, where they'll ask for a card number for the refund, leading to an account takeover.)

- You are about to be arrested by a scary 3-letter government agency. (They'll ask for gift cards, by having you read the numbers over the phone.)

False Authority Syndrome: Someone you've heard of says that a message is legit, important, urgent, or wonderful. Basically most advertisements with spokespeople, but with no actual permission from those people and companies to use their names. And now, with AI-created videos of faked celebrities.

FUD: Fear, uncertainty, and doubt. Used a lot in social media political messages, generally unsigned and unauthenticated, and trying to make the reader take action quickly, before thought kicks in.

Malware: Generic term for all bad software, because the old generic term 'virus' does not apply to most threats. A virus is embedded in a document or an image. Malware includes those, but most malware is a program or a script, not an infected document.

Smishing: A phish that arrives by SMS, a cell phone text message with a hoax link.

SpearPhish: Targeted bait, just for you. These messages include company-specific details to make your personalized message look legit. In years past, these mostly were sent to large company targets, trying to change payment locations for large financial transfers. Real estate settlement companies are given believable bank information for an upcoming settlement, but in the wrong country. There are urgent messages from the CEO requesting bank payments. Again, false urgency is added into the message.

Voice Cloning: Using an AI and a short sample recording, an AI can sound like anybody else. It was used in election robocalls in the New Hampshire primary, and is ready to use to leave a business voicemail asking for financial transfers to new (overseas) banks.

What AI Adds to Phishing

Just a year ago, most phish emails were easily identified as fake by watching for grammar errors, missing words, capitalization of common nouns, phone numbers that start with a ‘+’, and nonsensical errors like “pick up your package from *any* post office.” AIs can proof and fix such errors, or just write clean and individually-unique phish messages that spam email filtering won’t identify as bulk messages.

And targeting, for spear phishing, is getting better. The old error, of just using the domain name of the email as the name of the server and the company, will be replaced soon by simple online lookups of real company names and officers. That’s spear-phish lite, done entirely by an AI.

The number one security trend has always been this: Hackers look for security holes, either an error message in software, or employees that will literally click on anything, and they then try to turn that into a manual attack. Then they turn that into an automated bulk attack. And then it turns into a online service on the dark web, a ‘do it for hire’ service. AI will accelerate that. And since software is pretty-well patched, the soft target for AI-enhanced phish and spearphish will continue to be front-line employees who have not yet been shown what bait must not be taken.

More online:

Generative AI and Phishing
https://blog.lastpass.com/2024/01/generative-ai-and-phishing/

Deepfake scammer walks off with $25 million in first-of-its-kind AI heist
https://arstechnica.com/information-technology/2024/02/deepfake-scammer-walks-off-with-25-million-in-first-of-its-kind-ai-heist/

How AI is changing phishing scams
https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/how-ai-changing-phishing-scams

For computer help, call 410-871-2877
Missed a newsletter? Back Issues