TERRIFYING TECHNOLOGY TALES™

SPECIAL EVENT ISSUE

VOLUME 3, ISSUE 3.

VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

CONTENTS

Web of Destruction

It was a phishing email to one employee. But its ultimate target was thousands of inboxes. The large-scale attack worked when criminals accessed a user's Office 365 account and Contacts list, then cascaded a single phishing campaign into a web of devastating destruction.

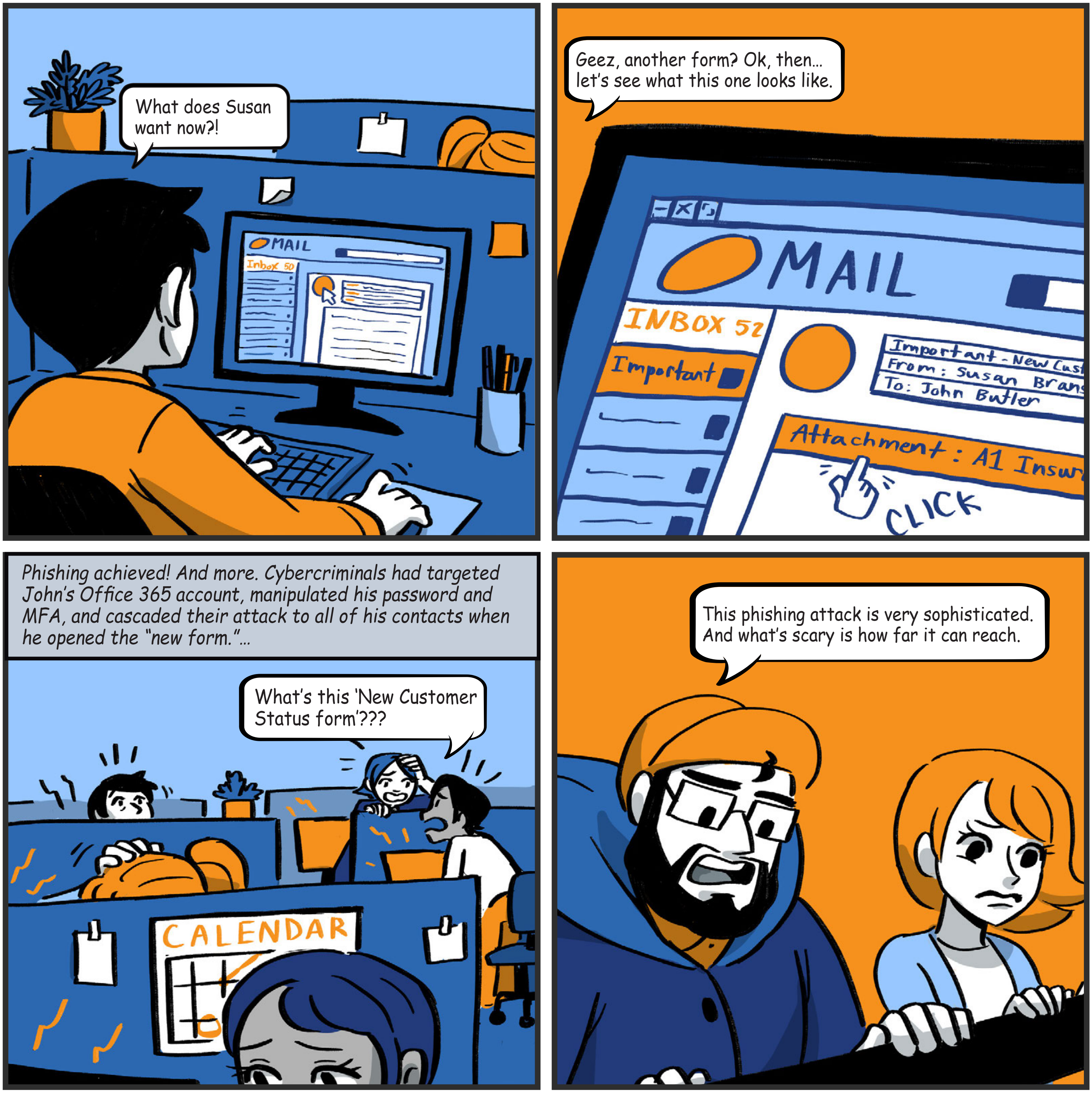
2023: A Chilling AI Odyssey

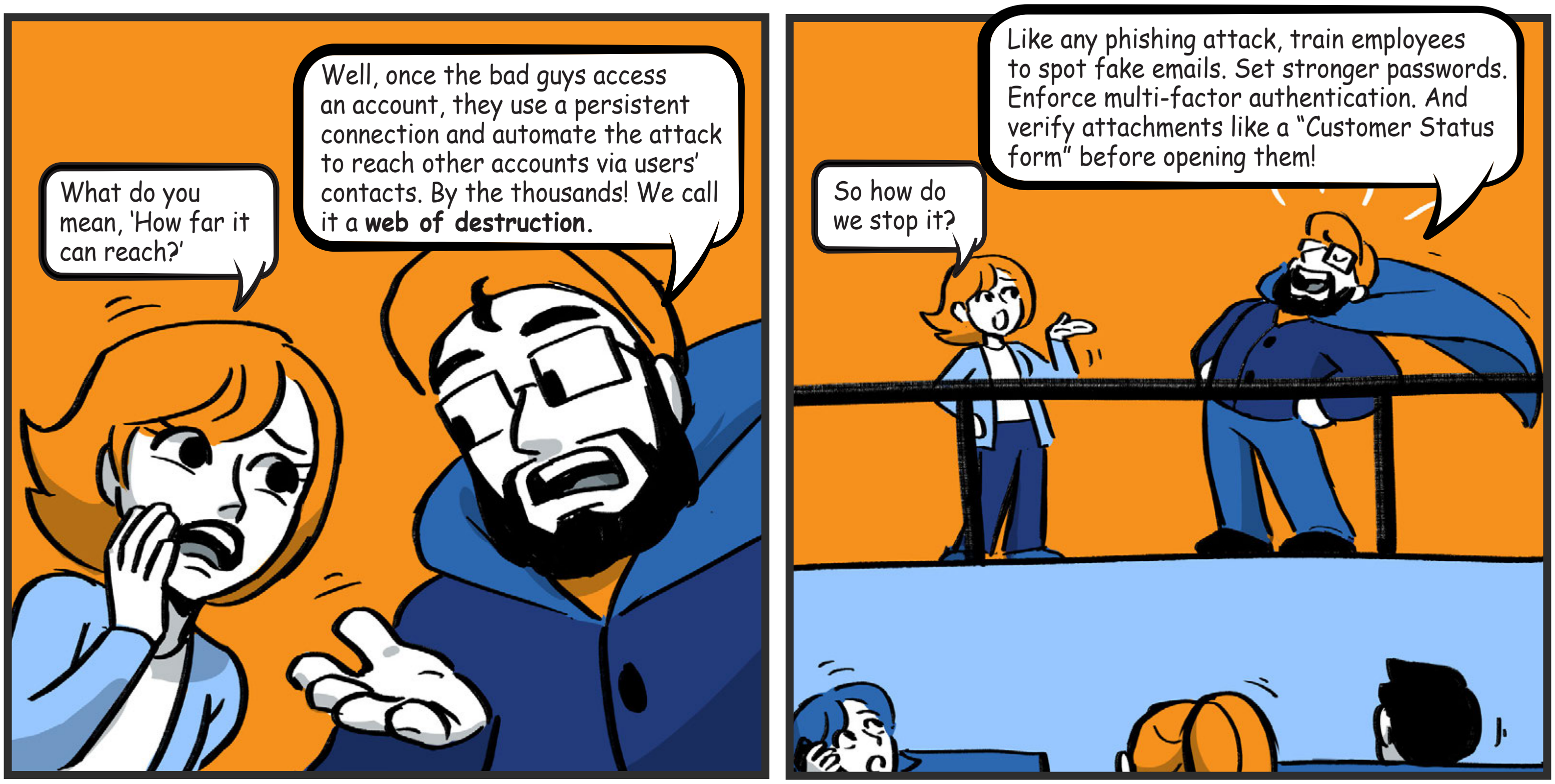
In 2001, it was a Space Odyssey with Hal the computer. In 2023, artificial intelligence is creating an odyssey of smarter malware, mass phishing, extortion, evading security protocols, and ingenious cyberattacks. In the hands of cybercriminals, AI isn't just dangerous — it's scary.

The Call is Coming from Inside the House

Virtually any infrastructure for IT and computing is a target for cyberattacks — wireless networks included. And if vulnerabilities exist, cybercriminals will find and exploit them. This isn't just "unauthorized access," it's an invasion of your organization.

Web of Destruction


What does Susan want now?!
MAIL
Inbox 50
Geez, another form? Ok, then… let's see what this one looks like.
MAIL
INBOX 52
Important
Important - New Cust
From: Susan Brans
To: John Butler
Attachment: A1 Insur
CLICK
Phishing achieved! And more. Cybercriminals had targeted John's Office 365 account, manipulated his password and MFA, and cascaded their attack to all of his contacts when he opened the "new form."…
What's this 'New Customer Status form'???
CALENDAR
This phishing attack is very sophisticated. And what's scary is how far it can reach.


What do you mean, 'How far it can reach?'
Well, once the bad guys access an account, they use a persistent connection and automate the attack to reach other accounts via users' contacts. By the thousands! We call it a **web of destruction**.
So how do we stop it?
Like any phishing attack, train employees to spot fake emails. Set stronger passwords. Enforce multi-factor authentication. And verify attachments like a "Customer Status form" before opening them!

IT SUPER KNOWLEDGE

START WITH THESE STEPS

Encourage employees to be vigilant against email phishing
Make sure users validate any email that's unexpected or appears suspicious, especially if it contains an attachment. Users should confirm the sender's email address, and be wary of a "legitimate" fake address. If a user is suspicious of an email or attachment, they should call or text the sender directly.

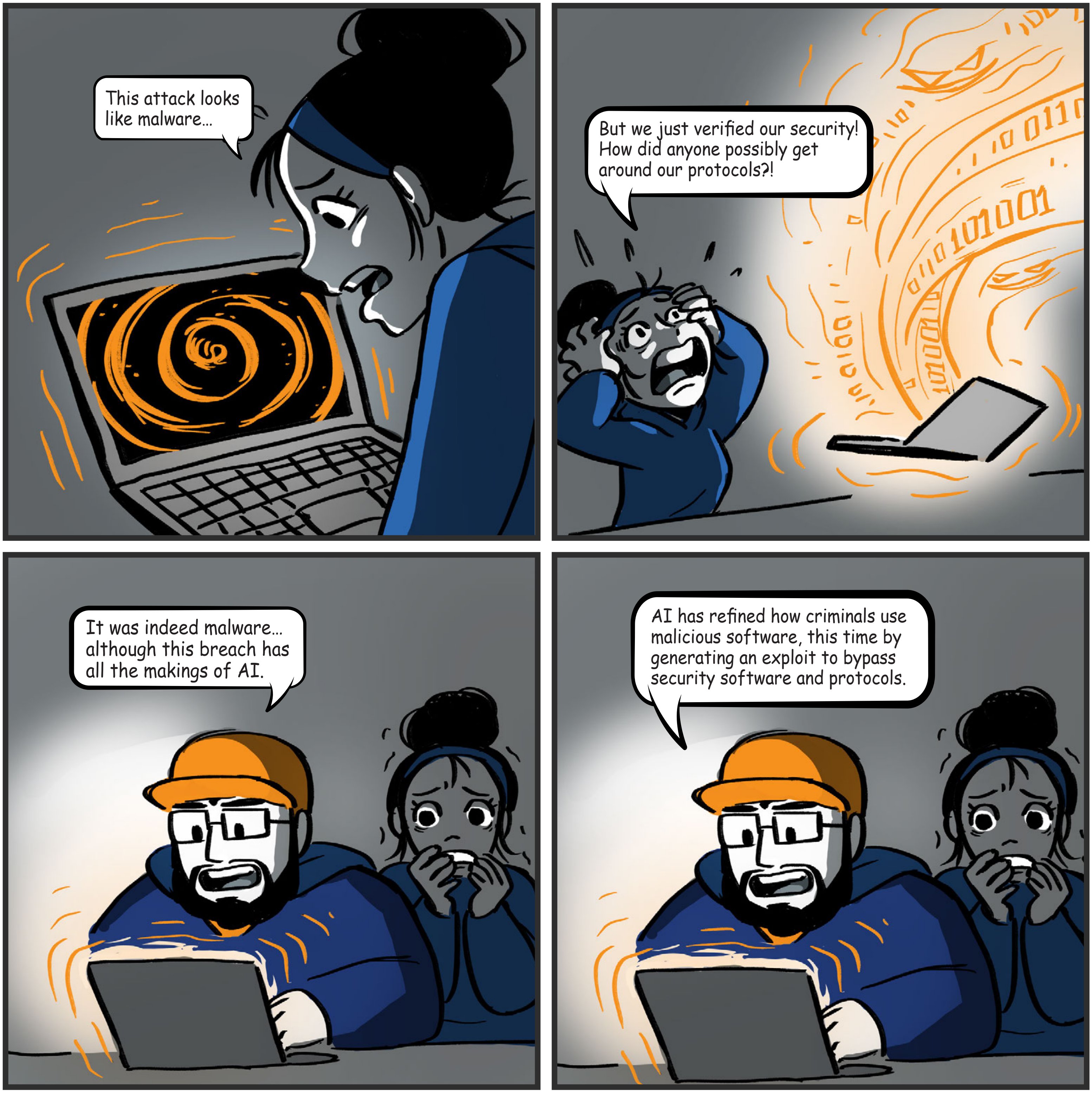
Take a deeper dive into cybersecurity training
Especially now with AI, criminals are making phishing more sophisticated and harder to detect. Beyond just suspecting a deceptive email, do your employees know how to verify an email source by server code, the sender's signature, and other means? Make this kind of training part of continuous cybersecurity education program for all employees.

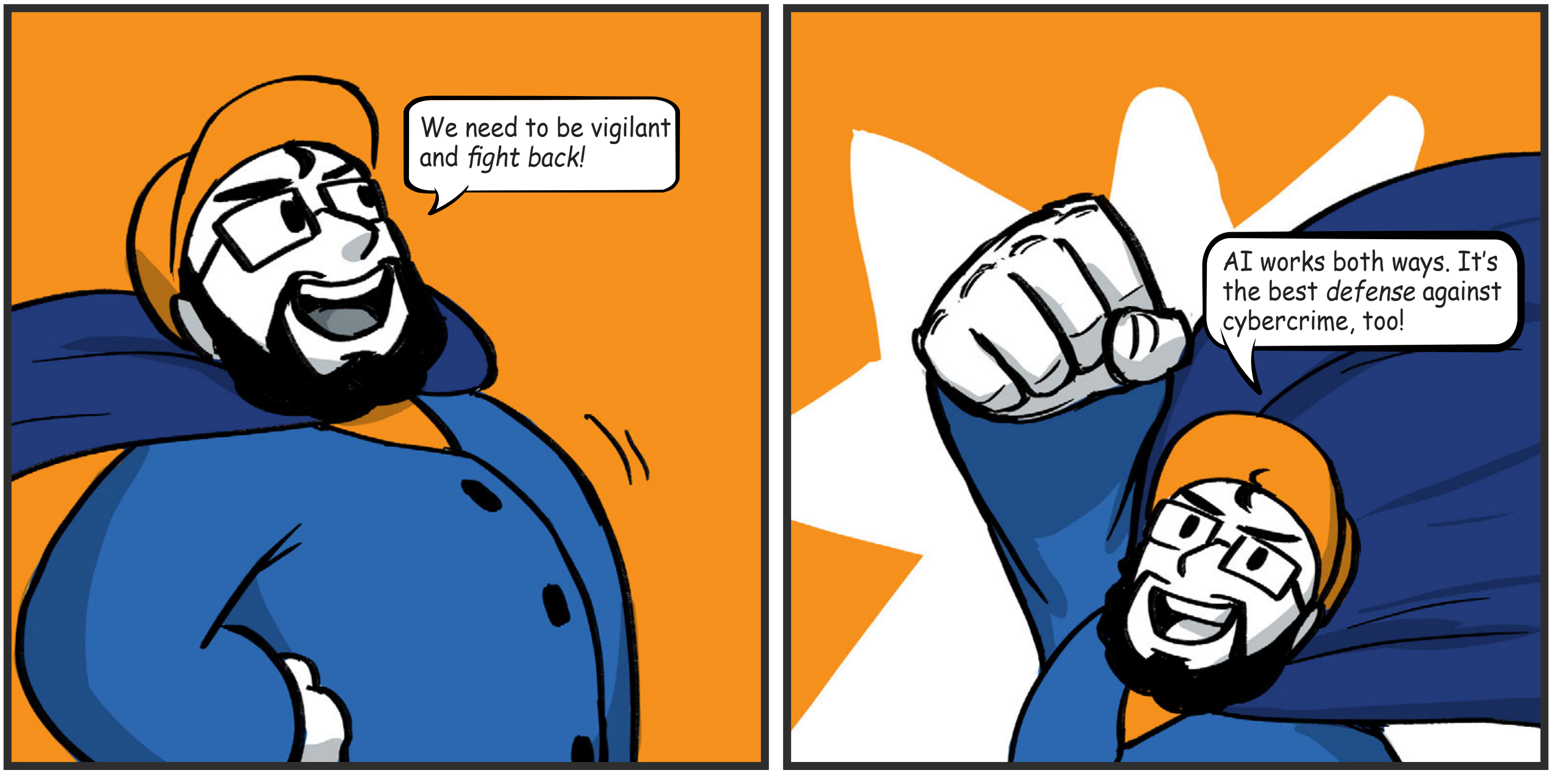
Be wary of certain words in email subject lines
Urgent. Important. Attention. Request. Payment. Invoice. New. Action. Required. These are just some of the commonly used words that can signal a phishing email. Make sure your employees know when to spot them.

To learn more about how to protect your organization, check out these additional resources.

- Protect Your Business from the Most Common Phishing Scams
- Security Breach: How Employees Can Help Minimize the Risk
- Password Management Best Practices Checklist

2023: A Chilling AI Odyssey


This attack looks like malware...
But we just verified our security! How did anyone possibly get around our protocols?!
It was indeed malware... although this breach has all the makings of AI.
AI has refined how criminals use malicious software, this time by generating an exploit to bypass security software and protocols.


We need to be vigilant and *fight back!*
AI works both ways. It's the best *defense* against cybercrime, too!

IT SUPER KNOWLEDGE

START WITH THESE STEPS

Learn how to detect AI-based attacks
For phishing campaigns for example, train users and IT teams to spot the difference between legitimate emails and web pages and ones generated via AI to trick potential victims.

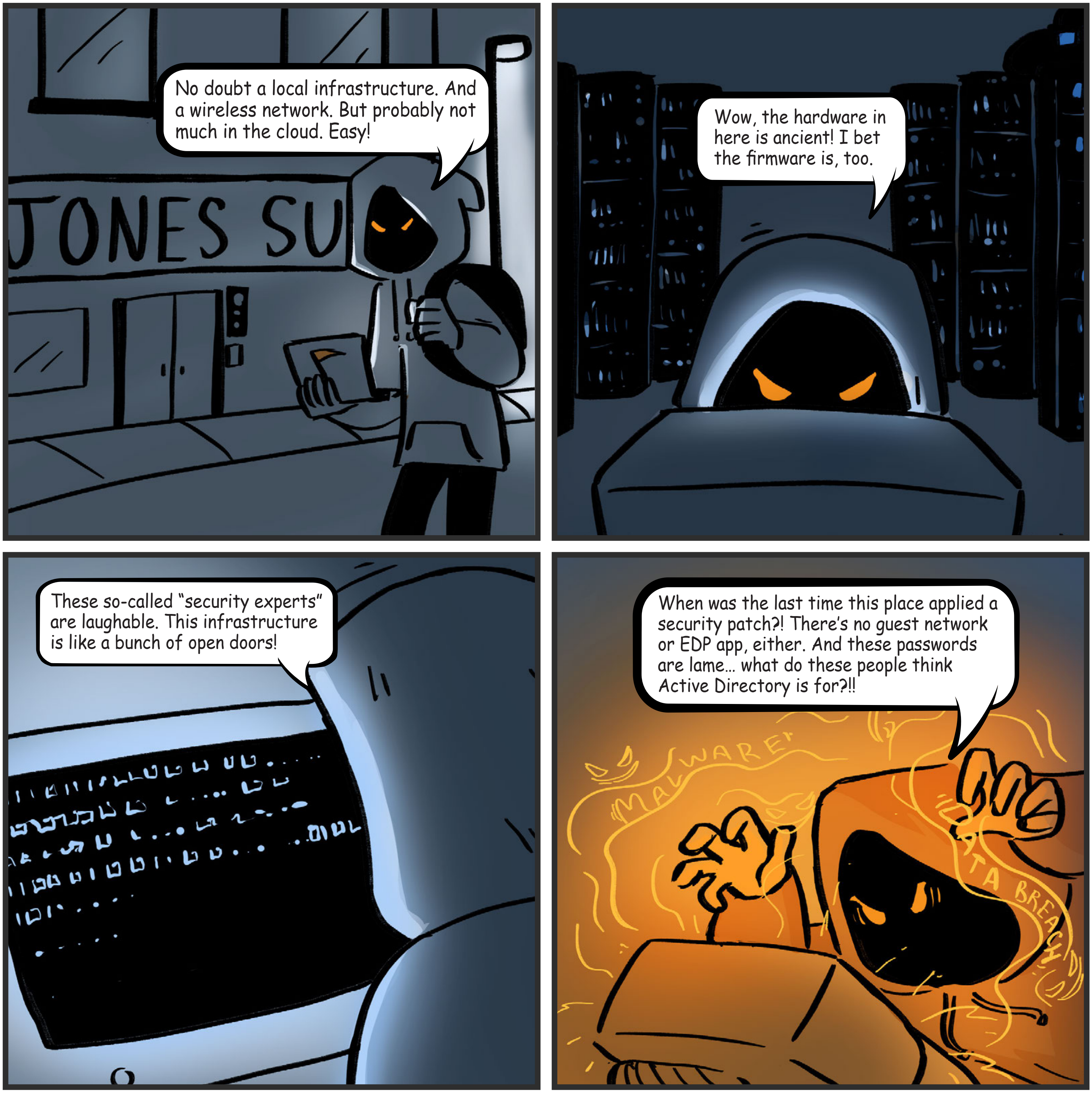
Remain vigilant… and use AI to fight back
Hackers are already getting around security walls with AI. Next could be cybercrimes like automated mass phishing, scripted malware attacks, and even extortion using harmful AI-generated images. AI tools can help detect known threats, identify new ones, audit data protection methods, and even scan massive amounts of data to forecast threats and detect attacks.

Conduct a security risk assessment focused on AI
A managed security service provider (MSSP) specializing in AI can pinpoint areas of your infrastructure that might be vulnerable to AI-based attacks — and then enhance your organization's security posture to include AI-oriented security measures for heightened protection.

To learn more about how to protect your organization, check out these additional resources.

- Preventing Cyber Attacks with AI and Machine Learning
- Technology Solutions: What You Should Know About Chatbots
- Information Technology Trends to Watch For in the Next Few Years

The Call Is Coming From Inside the House


No doubt a local infrastructure. And a wireless network. But probably not much in the cloud. Easy!
JONES SU
Wow, the hardware in here is ancient! I bet the firmware is, too.
These so-called "security experts" are laughable. This infrastructure is like a bunch of open doors!
When was the last time this place applied a security patch?! There's no guest network or EDP app, either. And these passwords are lame... what do these people think Active Directory is for?!!
MALWARE
TA BREACH

Ok, Jones Supply. I'm in your infrastructure, and now your network. It's like I'm in your house and you don't even know I'm here!
click
click
click
No, dude, we know you're here. And you're about to meet a *real* security expert. Your little invasion is over!

IT SUPER KNOWLEDGE

START WITH THESE STEPS

Audit internal infrastructure components
Ensure that hardware includes advanced security and vendor support, and replace any hardware and software that's reached an end-of-life stage. Also make sure vendor updates and patches are installed regularly, as soon as a vendor releases them.

Perform a security risk assessment
This helps determine what safeguards should be in place that currently are not; for instance, a robust endpoint detection and response (EDR) application to safeguard BYOD devices on the network.

Work with an MSSP to evaluate your security strategy
Measures like having security software and firmware in place are only one part of a security strategy. With a managed security services provider (MSSP) to help contrast it, a strategy should also encompass security needs such as data backup and recovery and even cyber insurance. Coordinating with an MSSP on a monthly basis also helps constantly address security for new attack types and vulnerabilities.

To learn more about how to protect your organization, check out these additional resources.

- Cybersecurity Checklist
- Quick Guide to Ransomware Defense
- Benefits of Partnering with a Managed Security Services Provider

Reach out anytime to ask a question or to schedule a no obligation IT security review.

www.visualedgeit.com
(800) 828-4801

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS