March 2023

inside zhero

CHAT GPT
A NEW PRODUCTIVITY TOOL ON THE LOSE

SOMETHING PHISHY
IS AI ADVANCING PHISHING ATTACKS?

WHAT'S HAPPENING AT ZHERO?

Message from Izak

Welcome to the March edition of Inside Zhero. This month, we delve into the underworld of cybercrime with a focus on phishing, the most lucrative form of social engineering.

Did you know that about 3.4 billion phishing emails are sent each day, and even the best security systems can't block them all?

IZAK OOSTHUIZEN
Bestselling Author,
Founder and MD

In this issue

Our feature article, "Don't Get Hooked," provides valuable insight into identifying and avoiding these dangerous emails.
Additionally, we take a closer look at the challenges facing the popular chatbots, ChatGPT and Bard, including privacy, legal, IP, and copyright concerns.

DON'T GET HOOKED

The stats are telling:

- According to IBM's Cost of a Data Breach Report, phishing was the most expensive attack vector used by malicious actors to breach IT networks in the past year, with an average cost of $4.9 million per breach.
- Phishing also accounted for 16% of all data and system breaches.
- In the UK, the Cyber Security Breaches Survey found that 83% of businesses that experienced a cyberattack in 2022 reported it as a phishing attack.
- Experts predict that by 2023, phishing could lead to the theft of over 33 million records.

Nuts and Bolts

Phishing attacks rely on users' naivety and trust. Just like the fishing homophone, attackers use bait to lure victims into clicking a link, giving away sensitive data, or downloading malicious software. There are two main types of phishing attacks.

- **Standard attacks** in which a large population of users are randomly targeted. While this method is haphazard, it only takes one victim to take the bait for the mission to be accomplished. Millennials and Gen-Zs are most likely to fall victim to these attacks.
- **Spear phishing** is a tactic that targets specific individuals or groups within an organisation using an email and an attachment. The email contains target-specific information and its level of familiarity is designed so that the victim or victims carry out the necessary actions needed to infect a network. Between 2013 and 2015 Google and Facebook were duped out of $100 million by Lithuanian fraudsters. The crooks created fake emails and invoices, pretending to be Quanta Computer, a Taiwanese hardware supplier to both tech companies. Both tech giants paid the bill.

Spotting the phisher

Most phishing scams aren't as sophisticated as the ones that Google and Facebook fell for. So, if you are vigilant, you can usually spot a spam email quite easily. Here are five tips to help you:

1. Legitimate companies always use their own domain name in their emails. For example, Amazon's emails will come from an address like **support@amazon.co.uk**, not **amazon.support@gmail.com**.
2. Check for misspelled domain names, like **support@ammazon.co.uk**.
3. Look out for poorly constructed emails with bad spelling and grammar.
4. Be wary of suspicious links or attachments.
5. Phishing emails often create a sense of urgency to make you panic and act quickly. Don't fall for it! Take your time, step back, and re-read the email with fresh eyes.

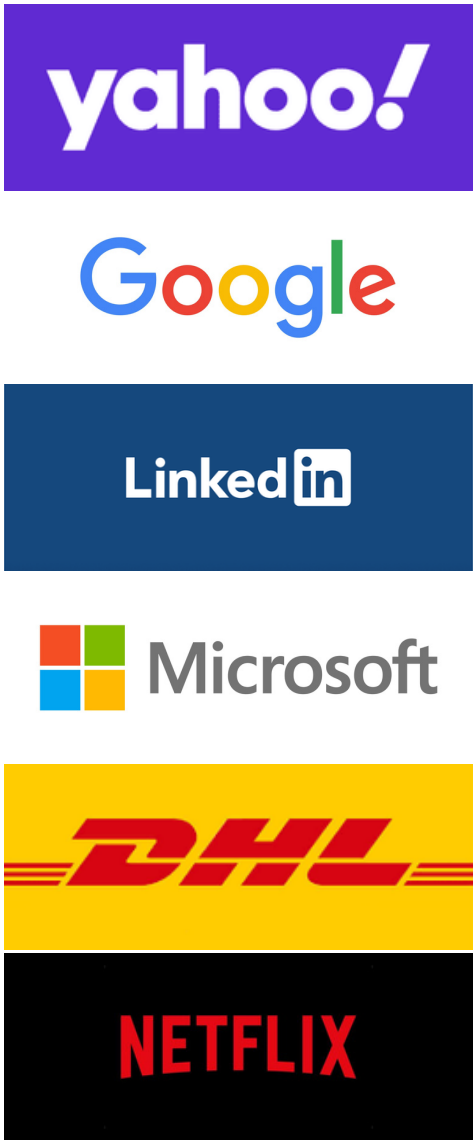
If an email looks suspicious, don't open it. If you do it by mistake, then never ever click on a URL contained in it. 50% of phishing websites make use of SSL certificates. Also, don't take your eye off the ball just because it's almost the weekend. A phisher's favourite day is Friday!

The most impersonated brands

In Q4 2022, these were the top brands ranked by their overall appearance in phishing scams:

1. Yahoo – 20%
2. DHL – 16%
3. Microsoft – 11%
4. Google – 6%
5. LinkedIn – 6%
6. Netflix – 5%

In 2021, PayPal held the top spot with Facebook coming in second.



No silver bullet

There isn't a silver bullet to prevent a phishing attack. On the technical side, you can implement Secure Email Gateways (SEGs) to monitor your employees' inbound and outbound emails, scanning them for malicious content.

To help curtail spear phishing attacks, you could deploy a cloud email security solution that uses AI and machine learning to analyse each employee's communication patterns and emails and establish patterns.

Train your team

Your team is the heart of your business, so you should start with them. Implement ongoing security awareness training and phishing awareness programmes which will have a massive impact on how your employees respond to phishing attempts.

New-school security awareness involves phishing simulation whereby realistic phishing emails are sent to your employees in order to gauge their awareness of attacks and their response to phishing emails when they receive them.

Phishing simulation platforms are offered by Mimecast, SoSafe, KnowBe4, and many others. Remember, prevention is better than cure. Get training and simulating now!

Phishing emails that disguise themselves as internal communications are especially concerning since they are sure to grab the attention of users and typically incite action.

New-school security awareness training for employees helps combat phishing and malicious emails by educating users on what to look out for.

Stu Sjouwerman,
CEO KnowBe4

A costly phishing timeline

2013
2015 GOOGLE AND FACEBOOK
$100 million

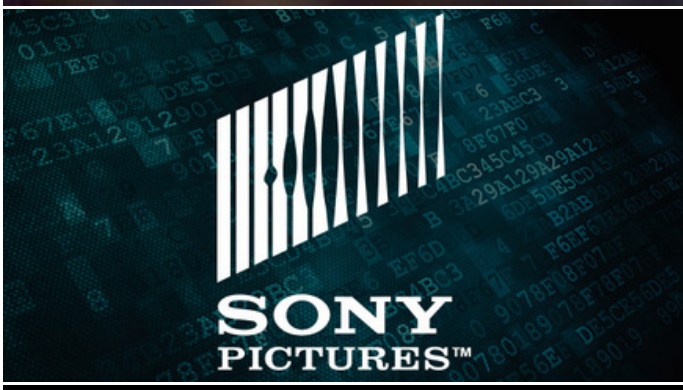
2014
SONY PICTURES
$80 million

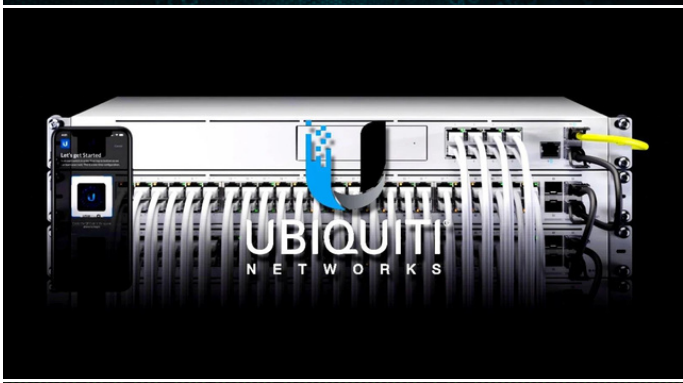
2015
UBIQUITY NETWORK WHALING ATTACK
$50 million

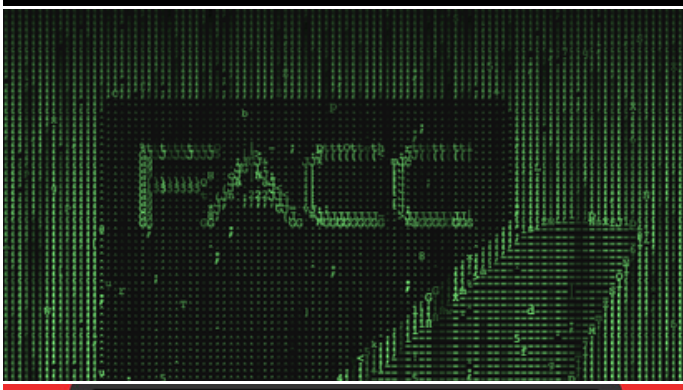
2016
FACC BUSINESS EMAIL COMPROMISE
$50 million

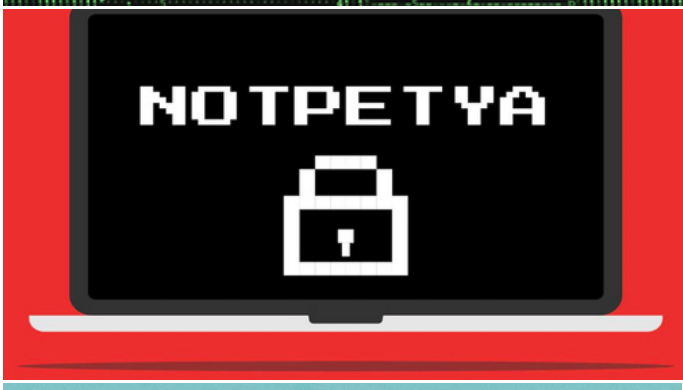
2017
NOTPETYA MALWARE
$10 billion

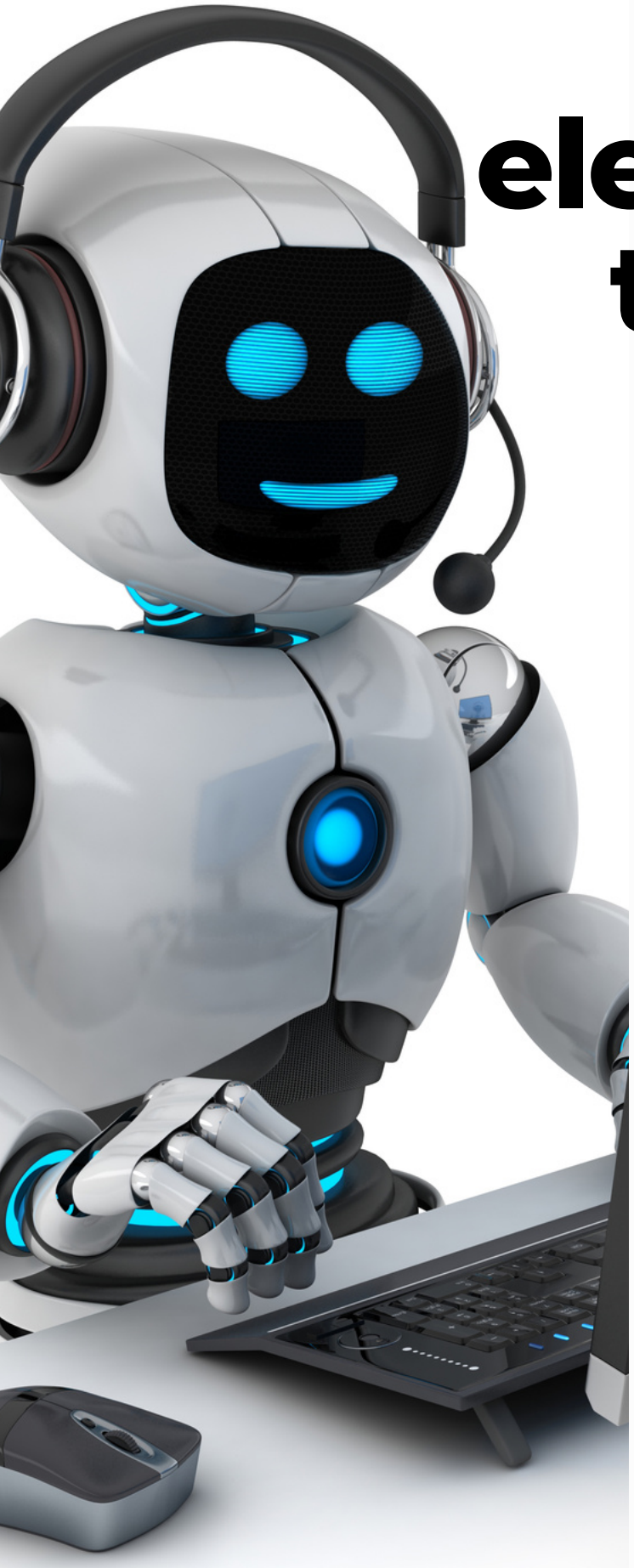
2021
COLONIAL PIPELINE
$4 million











The elephant in the room

Chatbot AI is a buzzword right now. Currently, with over 100 million users, OpenAI's baby, ChatGPT, has set the record for the fastest-growing consumer application in history. Microsoft has invested $10 billion in the technology, planning to integrate it into its ecosystem of products, including Bing and Microsoft 365. It even intends to use generative AI to train robots.

Hot on the heels of its competition, Google launched Bard, a chatbot based on its Language Model for Dialogue Application (LaMDA). But are ChatGPT and Bard as dazzling as they seem? Is there an elephant – or a few – in the room?

Factual inacuracies

A UK university student aiming for a first on an essay used ChatGPT to do the work. The result was a disappointing 2:2 grade. OpenAI has also admitted that its AI can produce biased answers and mixes fact and fiction. Alphabet, Google's parent lost $100 billion in market value on 8 February after Bard shared inaccurate information in a promo video.

But mistakes aren't the biggest problem. With ChatGPT and Bard, Microsoft and Google risk litigation and legal liability for every bit of misinformation their inventions create.

Data without consent

Is it too early to talk about AI and the law? Some say it's too late! All the content machine learning systems use was created by humans and crawled from the web. ChatGPT also hones in on your personal information obtained without consent. Were we asked by OpenAI if it could use our data? The straight-up is no. Some say this is a blatant violation of privacy, especially for sensitive data used to identify us, our family members, or our location.

OpenAI also didn't pay for the data it reaped. Nobody – individuals, website owners, companies or the government agencies that produced the content have been compensated.

Does that seem fair considering OpenAI's $29 billion valuation?

What about copyrighting?

Imagine ChatGPT has created some content that you love. So much so that you want to copyright it. You can forget it. At the moment, for work to enjoy copyright in the US or the UK it must be created by a human.

Even if the work could be copyrighted, what happens when ChatGPT generates duplicate or similar content for another user? Can the initial user sue others for copyright infringement? Margaret Esquenet, a partner at IP law firm Finnegan has this to say:

"Even assuming that the rightful copyright owner is the person whose queries generated the AI work, the concept of independent creation may preclude two parties whose queries generated the same work from being able to enforce rights against each other. Specifically, a successful copyright infringement claim requires proof of copying—independent creation is a complete defence."

A dangerous black box

ChatGPT and Bard seem tainted with concerns around data privacy, copyright and IP, compliance and even plagiarism. This situation is exacerbated by the fact that these chatbots operate on an input-output model. A user inputs a query and ChatGPT spews out a response. Even the experts at Microsoft and Google will be unable to predict the output. Put simply, nobody knows how these chatbots construct their outputs since neural networks are the quintessential black boxes.

Take this extreme example – a user asks ChatGPT for a remedy to an illness. The chatbot provides inaccurate information and the user gets sick. Again, who is to blame? An army of lawyers will provide the answer in seconds. Being able to identify a problem only after the fact won't be the best defence for Big Tech planning to implement public-facing generative AI.

We asked ChatGPT if it is dangerous. This was its split-second response:

"As an AI language model, I am not inherently dangerous. I am a software program created to respond to user input in natural language, and my purpose is to provide helpful and informative responses to the best of my abilities.

However, it's important to remember that I am only as good as the data and programming that have been used to create me. If I am programmed or trained to behave in a malicious or harmful way, then I could potentially be dangerous. But as long as I am used responsibly and ethically, I should not pose any danger to anyone."

WEBINAR

HOW AI IS REVOLUTIONIZING THE PHISHING LANDSCAPE

Picture this: a world where bots are smarter than humans, deepfakes are indistinguishable from reality, and your inbox is a minefield of malicious emails. Sounds like a nightmare, right? Well, welcome to the future of phishing!

Join the incredible Vin and Jamie for a one-of-a-kind webinar on Wednesday 29th March at 10am UK time, where we'll explore how AI is revolutionizing the phishing landscape, from the rise of chatbots to the terrifying power of deepfakes. But fear not fellow humans - we'll also teach you how to outsmart the machines and keep your online identity safe.

So grab your coffee and join us for an hour of witty banter, mind-bending tech, and expert advice on how to stay one step ahead of the bots.
Don't miss out!

Wednesday, 29 March
10:00 BST

Click here to reserve your spot!

ARE YOU THE ONE?

WE'RE HIRING!

Think you have what it takes?

We are always on the lookout for top talent. If you have what it takes to help us shift the dial up a notch, stay in touch for exciting opportunities.

Positions available:

- UK Onsite

Apply now

Meet the team

Chris Haverly

UK OFFICE MANAGER

1. What made you realise you want to go into the IT industry?

I love writing about almost any subject. When I had the chance to write about IT for Zhero, I jumped at the opportunity, knowing it would be a challenge that will allow me to explore the world of technology.

2. What's your most-used productivity tool?

I think it's my brain, but ChatGPT may be taking over at some point.

3. What do you enjoy the most about your role?

I love the variety the work offers and also collaborating with so many members of Team Zhero.

4. How would you describe yourself?

I'm easy-going, confident and playful. Some people think I'm shy but that's because they don't know me.

5. Do you have any hidden talents or hobbies?

I am a travel bug - I have visited about 30 countries. I also enjoy movies, music and cooking.

6. Are you a sports fan?

I follow ice hockey and tennis.

7. What is your favourite movie?

Gone Girl starring Ben Affleck and Rosamund Pike. I've watched it more times than I can count.

Speak to us
+44 20 7183 3975

London
162 Farringdon Road
London
EC1R 3AS