Read or listen to this article online

Scan the QR code to open this article on XO.PL

Article source:

https://xo.pl/it-made-fun-sec-phishing

IT SECURITY

Phishing: a letter from a bank that never sent it

At 8:03 on Monday morning, Agnes from Accounting opened her company inbox. The bank had apparently decided to freeze the company's account in nine minutes unless she verified her identity immediately. A huge red button was attached. The Manager walked past, spotted the word “URGENT,” and promptly upgraded the situation to a national emergency.

— AGNES! CLICK IT!

— Do you know where that button leads?

— TO THE BANK! IT HAS THEIR LOGO!

— I'll print you a police badge, then. You can start handing out parking tickets — Gregory called from behind his monitor.

The Manager stopped in his tracks.

— GREGORY, THIS IS NO TIME FOR JOKES. WE HAVE NINE MINUTES!

— Eight now. But the thief is running out of patience too, so perhaps we can all wait together.

A message from a bank that sent nothing

Agnes opened the message details. The displayed sender was “Bank Security Department.” The actual address looked like the bank's name after a fight with a keyboard.

— See? A display name doesn't prove who sent an email — she said.

— BUT IT HAS THE LOGO!

— Anyone can copy a bank's logo. Or its button colours, executive signature and photo of a smiling support agent.

Gregory pulled up a chair.

— This is **phishing**: trying to persuade someone to hand over information, money or access by pretending to be a trustworthy person or organisation. Email is only one possible delivery method. The deception matters more than the medium.

— So we're fishing for people? — Agnes asked.

— Exactly. Except a real fish doesn't get a text saying its fins need a security update.

— What should I do?

— Don't click. Don't reply. Go to the bank independently using your own bookmark, its official app or an address you've already verified. If there really is a problem, we'll check it there.

— Can I phone the bank? — the Manager asked.

— Yes. Using a number from its official website or your existing paperwork, not the number in the suspicious message.

Nine minutes until the end of the world

Three minutes ticked past on the wall clock. The Manager watched them like a rocket-launch countdown.

— What if it's a real warning? Why would someone lie about freezing our account?

— Because **time pressure** discourages checking — Agnes said. — People see “last chance,” “urgent delivery fee” or “unauthorised login” and want to act immediately.

— And what if it says I've won a million?

— Then they're hoping greed will do the job fear usually does. Different bait, same hook.

Gregory opened the genuine banking app. No warning. No freeze. The account carried on existing peacefully, entirely unaware that the world was supposed to end.

— Well, look at that. The bank is perfectly calm.

— CAN WE STAND DOWN THE CRISIS TEAM?

— Certainly. Although you've already ordered three pizzas for the team.

— THOSE ARE NOT CANCELLED.

The address looks familiar. That's the point

Gregory showed Agnes the address behind the button. It looked convincing until someone actually read the whole thing.

— The real bank's name might appear in the path, a subdomain or as part of a completely different domain. What matters is the actual destination host, not a familiar word somewhere in the URL.

— So seeing “bank” isn't enough?

— Calling a restaurant “The Embassy of Meatballs” doesn't make it an embassy.

— WHAT ABOUT THE PADLOCK? — the Manager asked. — A PADLOCK MEANS SAFE!

— **HTTPS** generally means an encrypted connection to a particular server. It does not establish that the owner is honest. Criminals can obtain perfectly valid TLS certificates too.

— Then why have the padlock?

— To help protect the connection from eavesdropping in transit, not to perform a character assessment of whoever runs the site.

— Like a sealed envelope sent by a crook?

— Exactly. We covered envelopes and postcards in our article about **HTTP and HTTPS**.

Gregory added that hovering over a link on a desktop can help reveal its destination, but phones behave differently, and previews or shortened links don't always tell the full story. The safer choice is not to follow a suspicious link at all.

A delivery nobody ordered

At 8:19, Agnes received a text: “Pay £1.49 to release your parcel.”

— I haven't ordered anything.

— BUT THAT'S A TINY AMOUNT! — the Manager observed. — WE CAN PAY IT FOR PEACE OF MIND!

— That's exactly what they're counting on. The link could lead to a fake payment page. The small charge is bait for card details or authorisation of a payment.

— Is that phishing too?

— Phishing by text is often called **smishing**. When someone phones pretending to be a bank employee or technician, it's **vishing**, short for voice phishing.

— So phishing has as many varieties as the Manager's catering orders?

— More. He always orders three pizzas.

— MAKE IT FOUR!

The bank calls to rescue your money

Right on cue, another call came in. A man introduced himself as a bank security specialist.

— We've detected a theft attempt. You must move your funds to a secure holding account immediately — he announced.

Agnes glanced at Gregory, who silently held up a piece of paper: “NO.”

— Please give me your name and staff ID — she replied.

— There's no time! Just read me the code from your text message!

— I don't share codes during unsolicited calls. I'm hanging up and contacting my bank directly.

The call ended. The Manager looked offended.

— BUT THE NUMBER ON THE SCREEN LOOKED LIKE OUR BANK!

— Caller ID can be forged too — Gregory explained. — That's **caller ID spoofing**. The displayed number doesn't always reveal where the call actually originated.

— SO I CAN'T TRUST MY OWN PHONE?

— You can use your phone. Just don't mistake its screen for a police-issued identity certificate.

A bank does not need your password, one-time code or a transfer to a supposedly “safe account” to rescue your money. End a suspicious call and contact the institution through an independently verified channel.

One invoice, one accountant, one very personal crook

That afternoon, an email arrived from a supposed supplier. This time the sender knew the company name, the Manager's surname and that Agnes authorised payments.

— That sounds more convincing — she admitted.

— Because this could be **spear phishing**: an attack tailored to a particular person or organisation — Gregory said. — The attacker may use public information, stolen correspondence or leaked data.

— And what if they target the chief executive? — the Manager asked, straightening his tie.

— Attacks against senior figures are sometimes called **whaling**.

— FINALLY, A PROGRAMME FOR EXECUTIVES!

— It's not a loyalty scheme, sir.

The email requested a change of bank details on an invoice. The amount was correct. So was the supplier's name. Only the account number was different.

— And that's why we don't verify these requests by hitting Reply — Agnes observed. — If someone's taken over the supplier's mailbox, we'd be asking the same criminal.

Gregory nodded.

— We verify payment-detail changes through a separate channel, using a previously trusted number. This kind of business correspondence fraud is often described as **BEC — Business Email Compromise**.

The Manager grabbed his phone.

— I'LL CALL THEM!

— Excellent. Just not the number printed on that invoice.

— BEING A HERO GETS HARDER EVERY DAY.

An “invoice” that really wants to be a program

Gregory pointed to another message. Its attachment had an invoice-like name, but the extension didn't resemble an ordinary document.

— What happens if I open it? — Agnes asked.

— That depends on the file and the defences in place. It might be an ordinary document, or it might exploit a vulnerability or try to run malicious code. Sometimes the danger isn't an attachment at all, but a link to a fake sign-in page.

— Are PDFs always safe?

— No. A file format doesn't guarantee safety. Neither does the word “invoice.”

— BUT WE HAVE ANTIVIRUS! — the Manager shouted.

— We do. Antivirus is a security guard, not a fortune-teller. We still need updates, sensible permissions and judgement. We talked about layered defence in **our security fundamentals article**.

Agnes reported the suspicious message through the company's incident process instead of forwarding it to everyone with the subject “CLICK THIS AND SEE WHAT HAPPENS.”

The second guard can be fooled too

— WE'LL ENABLE MFA AND THAT SOLVES EVERYTHING! — declared the Manager.

— We'll enable it because it helps enormously — Gregory replied. — But not all forms of **multi-factor authentication** offer the same protection against phishing.

— BUT YOU NEED A CODE AS WELL AS A PASSWORD!

— A criminal may trick you into sharing that code, approving a sign-in notification or handing over a session through a phishing site that relays the login. Some attacks let a user appear to sign in normally while a malicious intermediary captures access.

— SO TWO LOCKS AREN'T ENOUGH?

— Two locks are better than one. But if you invite the burglar inside yourself, the number of locks isn't the whole story.

Security keys and passkeys using mechanisms bound to the genuine website's domain can significantly reduce the risk of common login phishing. That's different from typing an SMS code into a stranger's website. It still doesn't prevent every possible scam.

— So I shouldn't approve a login prompt if I'm not signing in — Agnes said.

— Exactly. We'll cover passwords and that second security guard in “Passwords and MFA”.

A QR code is just a link wearing a square costume

Someone had left a printed sign at reception: “New guest Wi-Fi — scan the QR code to verify your account.”

— FINALLY! SOMETHING WITHOUT A LINK! — the Manager rejoiced.

— A QR code can contain a link — Agnes sighed.

— So the crook printed a link as little squares?

— Exactly. **Quishing** is a name for phishing through QR codes. Scanning one can open a fake website.

Gregory turned the sign over.

— And don't assume a sticker is official because the poster is in our building. Someone might have added the sticker later.

— SHALL WE BAN SQUARES?

— Let's begin by checking what we scan.

What if someone clicked anyway?

At 3:40 p.m., Agnes entered Gregory's office.

— I have a hypothetical question.

— Oh no. “Hypothetical” always means someone's already clicked.

— The Manager.

— ON WHAT?! — Gregory exclaimed.

— A special offer for free pizza for the crisis team.

The Manager appeared in the doorway.

— IT WAS A LIMITED-TIME OFFER!

— Did you enter a password, a code or card details? Download anything? Approve a login? — Gregory asked.

— ONLY MY NAME, EMAIL ADDRESS AND COMPANY PASSWORD.

Silence fell. Even the printer stopped pretending to work.

— Then we don't sweep this under the carpet — Gregory said. — Report the incident immediately. From a trusted device, change the compromised password, revoke active sessions where possible, and review the account's settings and access. If that password was reused elsewhere, change it there too.

— And if someone shared card details or sent money? — Agnes asked.

— Contact the bank immediately through its official channel to block the payment instrument or try to stop the transaction. If malware may have run, secure the device appropriately and have it investigated rather than continuing to use it for sensitive logins.

— SO I SHOULDN'T DELETE THE MESSAGE BEFORE ANYONE SEES IT? — the Manager asked.

— Exactly. Preserve incident information according to company procedures so we can determine what happened. Reporting quickly matters more than pretending it didn't.

— WHAT IF IT REALLY WAS JUST A PIZZA WEBSITE?

— Great. I'd rather investigate a false alarm than miss a real compromise.

After a click, the next action matters. Opening a page, entering a password, running a file and approving a payment are different events with different possible responses. There is no single magic procedure for every case.

The final fishing report

The next day, the Manager called a press conference.

— NEW COMPANY POLICY! WE TRUST NO EMAILS!

— That'll make invoicing difficult — Agnes observed.

— NO PHONE CALLS!

— That'll make talking to customers difficult.

— NO QR CODES!

— That'll make ordering from restaurant menus difficult.

Gregory stood beside the whiteboard.

— The point isn't to fear the whole Internet. It's to **separate a request from independent verification that the request is legitimate**. When someone demands urgency, passwords, codes, payments, changed account details or software installation, verify the request through a trusted channel.

— SO WE SHOULDN'T BELIEVE EVERY MESSAGE WITHOUT CHECKING?

— Particularly messages applying pressure or requesting something sensitive.

Agnes put down her phone.

— The pizza place just called. The Manager really did order four pizzas yesterday.

— FINALLY! SOME GOOD NEWS!

— Not entirely. They all say “payment on delivery.”

— GREGORY! CHECK WHETHER IT'S PHISHING!

— I will. But first stop giving out the company password in exchange for pepperoni.

The Committee for Safe Fishing reports: the fake bank received no transfer, the imaginary courier is still waiting for £1.49, and the supplier's real bank details have been verified. The Manager has a new password and instructions not to type it into pizza websites. His catering-order privileges have been suspended as a precaution. 🍕🎣🤣❤️