Becoming a Phish Fighter – Training to Spot Phishing Scams

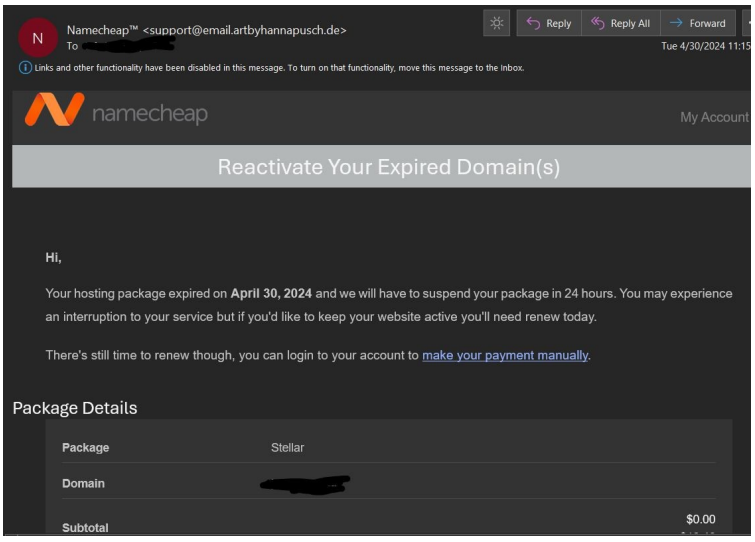
Author	josh
Date	2024-05-02

Overview

In this article, let's talk about fighting. No, I'm not talking about training martial arts with friends, but rather fighting a common and powerful cybersecurity threat – *phishing*. Phishing is a strategy used by hackers to trick *users* into giving up sensitive information – from account passwords, 2FA codes, payment details, or even cryptocurrency seed phrases. Systems can be fairly hard to break, but often *people* are much easier to trick. There are lots of tactics phishing scammers use to get sensitive data from their targets. Let's look at some *real* examples of phishing emails I've received, and analyze the tactics that these attackers use. By learning to spot phishing attempts, we can fight back and avoid compromise!

Common Phishing Tactics

Tactic #1 – Urgency



One thing that phishers love is *urgency*. Many of us are busy, balancing our work, hobbies, and families. When something urgent comes up, we often want that task *done* so we can get back to whatever important things we were doing before this chore presented itself. But urgency is a big *disadvantage* for security at times.

In this example, a phishing email contains an urgent warning that our Namecheap internet domain is expired. This means (if the domain is truly expired), that our users won't have access to our content anymore. For any website, this is of course a problem. This email states that in

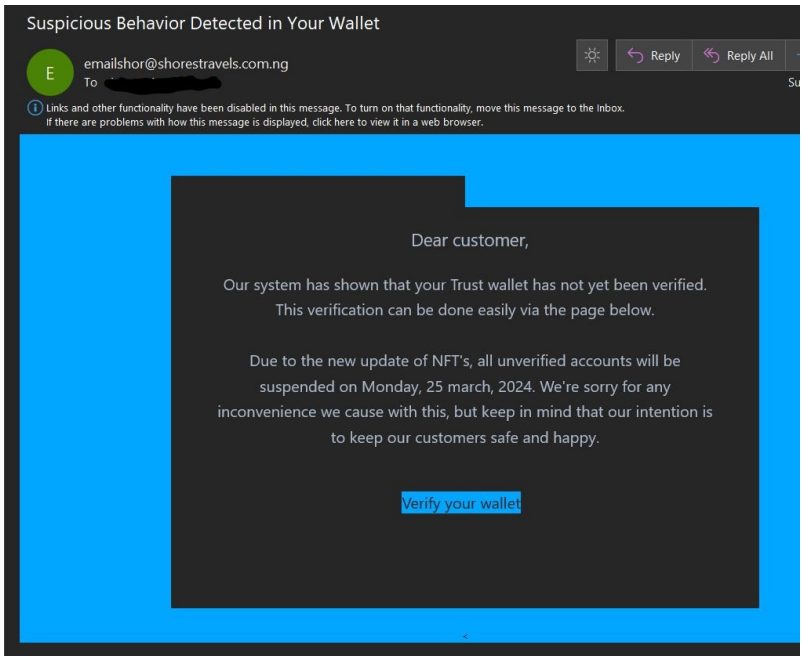
just 24 hours, and that I need to renew immediately to keep my website available. This example leads to a fake Namecheap *login form*, where the attackers can harvest my username and password!

I love this example in particular because *I almost fell for it*. Yes, phishing absolutely effects the cybersecurity aware too! I was in a hurry, and I thought that my Namecheap account had plenty of auto renewal funds. Nonetheless, I was alarmed and logged into my account to verify that my domains were, in fact, fine.

One particular phish-fighting tactics saved me in that case. First of all, I knew that I had some time and that, to my recollection, my account should be set up for auto renewal. So something already felt off. This triggered my hesitancy to follow any links *from the email itself.* Instead of clicking the link in the email, I went *directly* to `namecheap.com` and checked. Had I clicked the link and entered my password into the fake form, I could have had my password compromised.

Another helpful tip that made me aware of this phishing scam was the *source* of the message. This isn't always easy. In this case, the attackers didn't even bother to change the *from* field of the email to match the purported source (something like `support@namecheap.com`). The email this came from is someone's (presumably compromised) business email. Sometimes, this from field can be *spoofed* by the attackers to match the expected account, so if something feels off you can view the actual email headers to see the real source. This is a bit more technical, but useful if you learn how to do so.

Tactic #2 – Threats



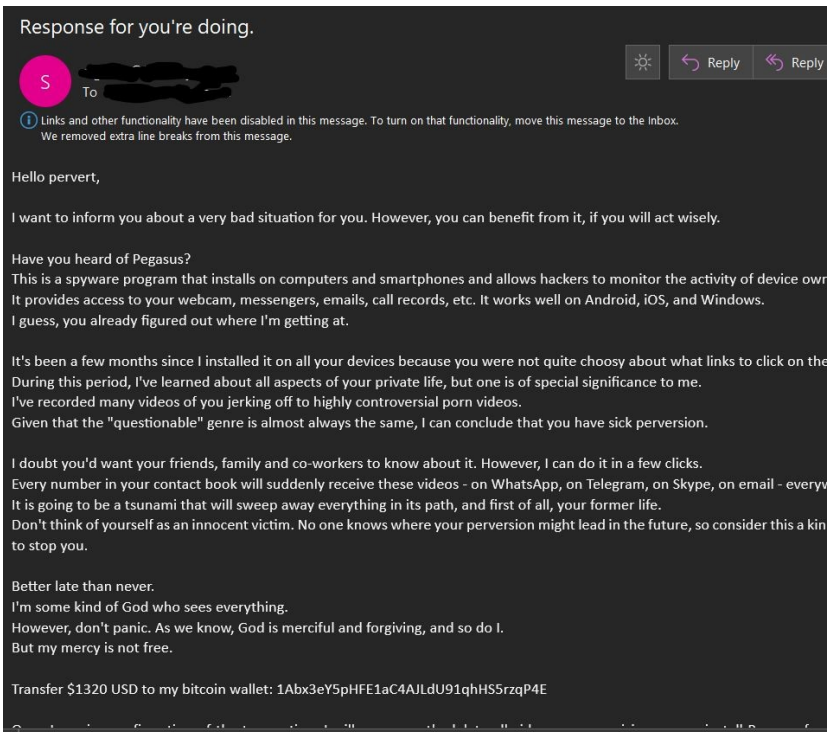
Another tactic phishing attacks commonly use is somewhat similar to that of *urgency*. *Threats*

that they will do something you don't want can trick you into panicking and giving up what they want. *Threats* often come with *urgency*, because if you're scared *and* in a hurry, you're less likely to take time and think about whether that threat is actually legitimate.

In this example, the user receives a threat that their Trust Wallet will be deactivated, and that they will no longer have access to their cryptocurrency assets. Nobody wants to lose access to their money (especially if you have a lot in one place), and so this threat often works. The link leads to a form that asks the user to enter their wallet *seed phrase*, which will grant the attackers access to *all of the money in that wallet.* Keeping your cryptocurrency seed phrase private is of critical importance – it's the keys to all of your coins.

In this case, a helpful phish-fighting tactic is to *evaluate the threat* rationally. First of all, I don't even use Trust Wallet currently, so this threat makes no sense. But let's assume that I do. This email says that my Trust Wallet will be *suspended* if I don't comply. But Trust wallet is not an exchange, it is a *non-custodial* crypto wallet. With this type of wallet, the user has a *seed phrase* and ultimate control of their coins. Because the user has their keys, they can always transact on the blockchain without approval from any 3rd party whether they are using Bitcoin, Ethereum, Bitcoin Cash, Litecoin, or some other *decentralized* coin. Only an exchange account (a *custodial* wallet) can stop users from sending funds because they control the keys. It's impossible for any non-custodial wallet to "suspend" a user – they could just import the keys into another wallet if they tried.

By taking time to evaluate the threat, we realize that it is an empty one, and simply a trick to part us from our seed phrase (and therefore our money).

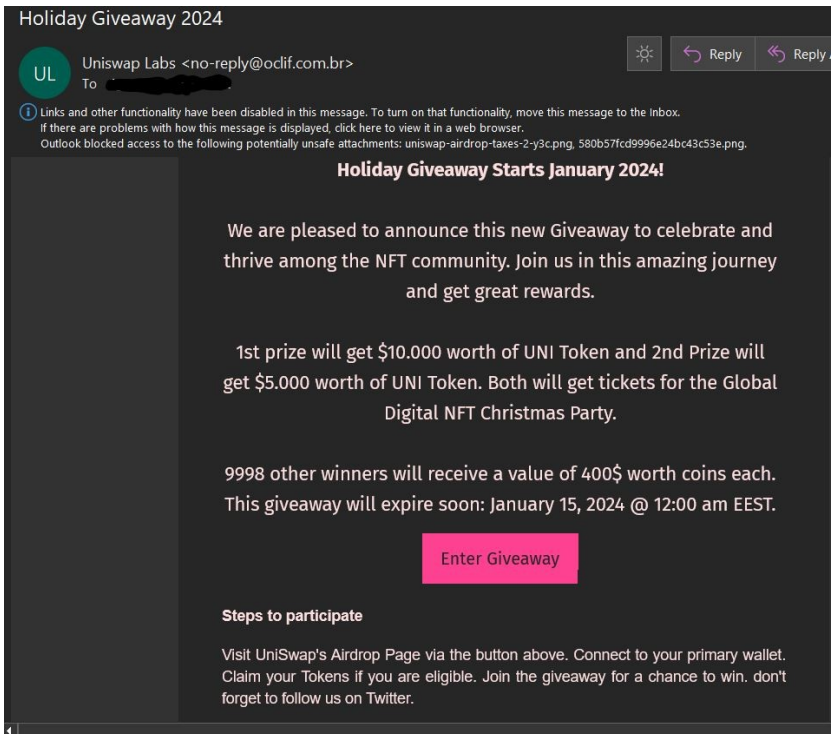


Threats can also take on a legal or social nature, and these type of threats are often effective as well. This second threat example tries to convince a user that they are about to have their lives upended by some embarassing socially-stigmatized revelation. In this case, the attacker claims that they have complete control of a user's machine: software, contacts, data, and camera. The attacker claims to have recorded embarassing footage of you and that they will share that with your social network unless you *pay them*. This creates a threat and a sense of urgency to alleviate that threat, along with a clear path to give the attacker what they want and stop the threat. You have to pay them in Bitcoin (or another cryptocurrency) which is global, decentralized, and *irreversible.*

In this case, again, it is important to both slow down and evaluate the threat. It's pretty unlikely that this attacker actually has full access to your computer. Modern operating systems and antivirus software is pretty good, and malware proliferation doesn't usually happen through most of the legitimate websites you visit. Not foolproof, but pretty good. Second, you may not do the embarassing thing that the hacker is threatening you with.

And finally, even if an attacker did have full access to your PC, your browsing habits, and your contacts, they probably aren't going to threaten you and ask for a relative pittance in Bitcoin. It would be easier, more effecient, and more discreet to just steal your passwords for bank accounts and cryptocurrency exchanges or wallets and steal everything they can that way. Why bother asking you? In this case, they're asking because they don't actually have any access at all, they just sent an email (which anyone can do) hoping you'll panic and send them an irreversible form of payment.

Tactic #3 – Rewards



If the threats and urgency don't get you, a juicy *reward* just might. Who doesn't love free money? Cryptocurrency airdrop scams are a profitable tactic for phishing scammers to part victims from their valuable coins.

In this example, the email offers several thousand dollars worth of Uniswap (Ethereum-based) tokens. The user can click "Enter Giveaway" for their reward. These scams usually follow one of two paths. One is to ask the user to send some amount of coins to "verify" their wallet, and receive double that amount back. Instead, the attackers simply steal the coins you sent. Crypto transactions are irreversible, so there is no way for victims to do a chargeback. The second option is to use a feature of Ethereum-based wallets called "WalletConnect". This tool allows users to interact with and sign smart contracts and transfer tokens. In the case of these phishing scams, the users are tricked into signing a malicious transaction that empties their wallets, sending those coins to the scammers.

The tactic we can use to fight these scams is to evaluate if the reward is *too good to be true.* Does someone really want to send me $10,000 for free? Unlikely. As well, is that person likely to send out random emails to unexpected recipients? A legitimate giveaway won't ask for private information or money in advance. In cryptocurrency, it's especially important to think about the consequences. Never send money to get money, as transactions cannot be reversed. Never sign a random, unknown smart contract.

Phish Fighters: You Should Train Too!

Scammers, hackers, and attackers of all stripes love to use phishing for their ends. Again, *people* are easier to break than *systems* in most cases. Scammers love to use urgency, threats, and rewards to their advantage. Luckily, we have some counter-strategies to fight these phishing attacks:

- *Slow down* – Take the time to go directly to the website in question instead of clicking on a link in the email. Think critically about the situation at hand – is it truly likely you must act now prevent losing access to an important resource?
- *Consider the source* – who did this email actually come from? Is it from some random account, or the actually expected site. Look at the email headers if technically able, and again, always go directly to the resource rather than clicking on links in the email
- *Evaluate the threat* – Take the time to think if a threat actually makes sense. Is it truly likely that someone gained full access to your devices? Can a non-custodial wallet provider actually lock my funds? Taking your time to evaluate threats can save you from a panic-induced mistake
- *Be wary of too-good-to-be-true rewards* – Most people, although good, are not so altruistic as to send random strangers thousands of dollars. As well, think critically about what they are asking for. Nobody should ever need *private* information or *money* to give you money. If someone is asking you to send cryptocurrency, sign a smart contract, or enter a seed phrase to give you money it is a scam.