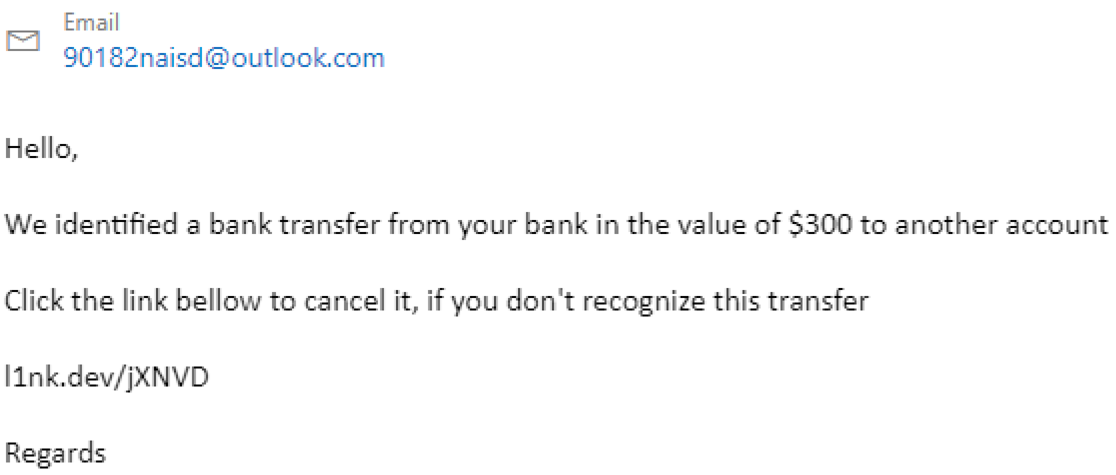
1. Phishing



Email
90182naisd@outlook.com

Hello,

We identified a bank transfer from your bank in the value of $300 to another account

Click the link bellow to cancel it, if you don't recognize this transfer

l1nk.dev/jXNVD

Regards

- Phishing is a form of attacking the victim using social engineering. The attacker may try to extract information or even money from the victim. The attacker may also try to infect the victim's machine with malware.
- One of things to pay attention to when receiving an email, message, or other type of contact, is to **check the sender**.
  - Check first, if you know the email and name of the sender;
  - If not, check if it is a suspicious address, like random characters or words that don't make much sense with the context. Example: the sender says he is from Bank X, but the email address doesn't belong to the Bank X domain;
  - Check the name of the sender, even that it can be easily changed to a trustable name;
  - Check for the e-mail address online, it may be or some warning list for suspicious emails, or if it is from a real company, it may appear on the company website.
- Never download or execute files if you're not sure what they are or who sent them, it may contain malicious softwares.
- For the same situation, don't click links either. They may also contain malicious softwares, or redirect you to a malicious website, or even a fake website that reminds you of a legitim one.
- **Reconnaissance**: Process done by the attacker to gather information about the victim, so he/she can make the phishing attack more believable and have more chances of success.
  - Check the victim's social media, where he/she works, etc
  - For example, if the attacker knows where the victim studies, or work, or places he/she goes, it's easier to come up with a more believable story.

1.1. Some techniques used on Phishing attacks to make the message more believable

1.1.2. Typosquatting

A type of URL hijacking, the attacker creates a fake website almost or identical to a legitim one, and with a URL address also very similar to the real one.

The fake website will have only a word or some very small differences from the original one, this way an user can access the website by accident by mistyping the real website URL, or receive the website's address and doesn't pay attention to the small differences.

Example:

Original website: www.google.com

Fake website: www.goegle.com

1.1.3. Prepending

The attacker will use expressions on the email to make it look more trustable, like "MAILSAFE:PASSED", "RE:RE"

1.1.4. Pretexting

The attacker pretends to be someone else to extract information from the victim: "Hello, I am from the hospital Y, please inform your home address so we can complete your file register"

1.2. Types of Phishing Attacks

1.2.1. Pharming

Pharming is a type of attack where you attack an entire group of people. For example, if the attacker wants to attack clients from a specific fast food's clients, he or she can **Poison the DNS Server** from the fast food's website, that way, all the customers that try to access the website will be redirected to an identical malicious one. As the bogus website can be almost identical to the original website, it's hard even for the antivirus to detect the fraud.

On Pharming attacks, the attacker performs a mass attack, like poisoning the DNS Server, instead of attacking each individual at a time.

- How would phishing and pharming work together?
    - **Phishing** - stealing credentials with social engineering
    - **Pharming** - mass attack
    - Example: The attacker poisoned the dns server from a legitim website, the user access the website and fills a form with his address information to receive a product.

1.2.2. Vishing (Voice Phishing)

Vishing or Voice phishing, is a phishing attack that is done through a phone call or voice mail.

The attacker may use a technique called **Caller ID Spoofing**, where he spoofs the phone number he is calling from, so it may look like a call from someone nearby.

1.2.3. Smishing (SMS Phishing)

Smishing is when the phishing attack is done by SMS / text message. Caller ID Spoofing can also be used in this attack.

1.2.4. Spear Phishing

Spear Phishing is when the phishing attack is targeted to a specific person or a specific group of people. For example, an attacker can target the financial team from a company to convince them to transfer money to him/her.

1.2.4. Whaling

Whaling is the type of phishing that aims for "high-ranked" people, like CEOs, senior executives, etc. Whaling it's also known as CEO fraud.