How to protect yourself from phishing scams?

I guess you've also felt an increase in fraud attempts lately, either through phone calls coming from numbers across Europe and the world, selling stocks, cryptocurrencies or wanting to fix online services you don't even use, or via e-mail, from traditional mass messages sent by "Nigerian princes", to carefully planned man-in-the-middle attacks on your company or organization.

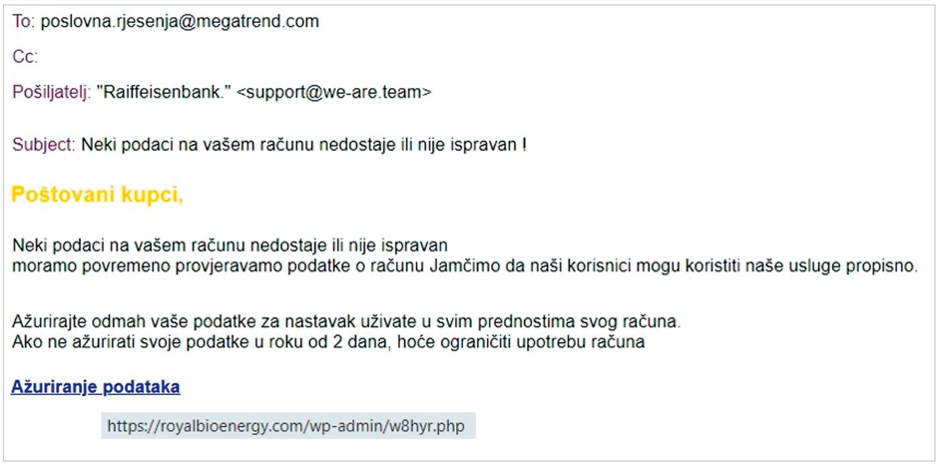
Author: Domagoj Marić

Phishing is one type of such online fraud, where the ultimate goal of the attacker is illegal financial gain - to steal money, or data, which in turn ultimately results in the victim's loss of money. Such scams are probably as old as the Internet, while attackers have become very sophisticated in their methods over the years. The whole situation has worsened in the last few years with the arrival of several periods of lockdowns, where people were forced to stay in their homes and often spent more time on computers. Therefore, those who are not accustomed to using computers frequently had to adapt to more digitization, and with increased digitization comes greater exposure to fraudulent e-mails.

PHISHRBAN PROJECT

Therefore, Megatrend poslovna rješenja has contracted a grant to increase the development of new products and services resulting from research and development activities - Phase II, funded by the European Regional Development Fund (EFRD), for a project named "Research of natural language processing (for Croatian) and the development of the PhisHRban product to increase cybersecurity".

The project is implemented by Megatrend poslovna rješenja d.o.o. as a Project Beneficiary together with partners - Faculty of Philosophy and Faculty of Economics, University of Zagreb, and the project aims to develop a new, innovative product PhisHRban that will enable the recognition of phishing messages in Croatian to increase cybersecurity using natural language processing.



To: poslovna.rjesenja@megatrend.com

Cc:

Pošiljatelj: "Raiffeisenbank." <support@we-are.team>

Subject: Neki podaci na vašem računu nedostaje ili nije ispravan !

Poštovani kupci,

Neki podaci na vašem računu nedostaje ili nije ispravan
moramo povremeno provjeravamo podatke o računu Jamčimo da naši korisnici mogu koristiti naše usluge propisno.

Ažurirajte odmah vaše podatke za nastavak uživate u svim prednostima svog računa.
Ako ne ažurirati svoje podatke u roku od 2 dana, hoće ograničiti upotrebu računa

Ažuriranje podataka

https://royalbioenergy.com/wp-admin/w8hyr.php

A schoolbook example of a phishing message

Within this project there are two basic components (problems, challenges) that we must solve in order to achieve this goal - the first is the detection of phishing e-mails, while the second is the detection of malicious phishing URLs, which most often lead to fraudulent and malicious sites, which aim to deceive the victim by stealing money or sensitive data.

HOW DO ATTACKERS GET YOUR MAIL ADDRESS?

There are four basic ways for attackers to get your e-mail address, which is usually just one of hundreds, thousands, or even millions of e-mail addresses:

- buying a list of e-mail addresses (called paste or dump) - often a set of several million addresses, so attackers send one message to all of them
- collecting e-mail addresses by searching the web (e-mail harvesting) - collecting addresses using web crawling scripts and basic regular expressions for e-mail addresses
- fake websites, which attackers set up to collect sensitive victim data (a lighter version of phishing that allows for other phishing scams to happen)
- data breaches - Facebook, Yahoo, Dropbox, LinkedIn, MySpace, Adobe and Snapchat are just some of the victims of data breaches, so we need to be careful where we leave our personal data

WHAT ARE THE BASIC TYPES OF PHISHING ATTACKS?

The first and most primitive type of phishing messages are fake, i.e. non-existent prize games (giveaways). With the notification that you are the winner of the prize game, you are usually instructed to click on the suspicious URL address or download the attachment. Of course, the general rule here is that if you don't sign up for any of it, you won't win anything, and even if you did sign up, double-check the notification you received. A variation on this message is still a very popular fraud of a non-existent order, where the recipient receives a seemingly legitimate notification about the execution of an order that he did not make, but it is still about malicious links or attachments.

One step above in the spectrum of primitiveness of phishing scams are the traditional messages of “Nigerian princes”, where the sender claims that he comes from a third world country and needs your help in the transaction of his wealth. In most cases, this is followed by instructions for the payment of a certain “initial” amount (confirmation fee), after which the victim no longer hears from the attacker. Since this type of scam is almost as old as e-mails, there are many variations with the same goal.

The average Internet user today uses a large number of different online services, be it multimedia services for streaming music and movies, e-mail services, physical mail or online shopping platforms, which is why there are obviously many frauds associated with accounts of such services. In such malicious messages, the subject is most often a subtle warning to the user that he must make a payment in order to continue using the service (and often a direct threat of termination with an additional dose of urgency). These messages have the same goal and method as the previous types, so you should definitely check the grammar and spelling, as well as the URLs of the links, so that you don’t end up on fake pages.

The last, and at the same time the worst type of phishing fraud is spear phishing, which is the biggest problem today. In such a scam, the attacker is well aware of the nature of communication between two people (who those people are, what their relationship is, what their role is in an organization, etc.), so he intrudes into the conversation using a fake but seemingly legitimate e-mail address. This is the most sophisticated method of attack, and is most often targeted at companies and organizations. Some quick payment, access to a system or sensitive information is required. Since this type of phishing message is very diverse and depends on who the victims are and what exactly the attacker wants to achieve, there is no universal advice other than to always be skeptical and double check every suspicious item of the message.

HOW TO DETECT A MALICIOUS URL ADDRESS?

In the end, the obvious question is how to know when to stop before clicking on a link. What should always be kept in mind is the concept of the semantic web - website URLs should be semantic, meaningful and readable. For example, it makes sense that the URL address of the Megatrend blog page is megatrend.com/blog, as it contains exactly the information it should contain. Malicious URLs are most often the exact opposite of this concept.

If you want to learn more about the application of artificial intelligence in the field of information security and specifically in solving the problem of detecting malicious messages on the Internet, contact the experts of Megatrend poslovna rješenja at poslovna.rjesenja@megatrend.com.

MAIN CHARACTERISTICS OF PHISHING MESSAGES

- mentioning money and/or (crypto)currencies, e.g. EUR, bitcoin...
- generic greetings
- lots of IT and law terminology which doesn’t make much sense
- urgency, warnings and threats of termination, short deadlines to react
- bad grammar and spelling (bad automated translation)
- mail address is not legitimate and so called doppelgänger domains, e.g. domagoj-megatrend@scammer.com instead of domagoj.maric@megatrend.com
- suspicious URL addresses, suspicious and unexpected attachments (e.g. zip archives which can also contain malware)
- mentioning named entities such as famous companies and services (e.g. UPS, PayPal, Facebook, Netflix...)

http://megatrend.com-useridweb12347861257.scammer-domain.com/app/76322

protocol	http://
domain	scammer-domain.com
path	/app/76322
subdomain 1	com-useridweb12347861257
subdomain 2	megatrend

The structure of a URL address on an example of a phishing address

MAIN CHARACTERISTICS OF PHISHING URL ADDRESSES

- unnecessarily long, large number of digits
- visible extensions and ports
- keywords (pay, shop, secure, login, verification)
- a name seemingly similar to a popular site (PAYPAI, Faceb00k, rnicrosoft...)
    - ○ character substitution -> homograph attacks
- a large amount of subdomains
- a large amount of additional parameters after the path
- long strings of alphanumeric characters without lexical meaning or hex characters
- www domain prefix (e.g. “www702.paypal.ca”)