Phishing Campaigns

We all use at least one email address, no matter our day-to-day profession. Thus, the majority of attack vectors use it for fraudulent reasons from stealing credentials to gain access to your computer or phone; such emails are known as “phishing” emails. There are two types of malicious campaigns:

1. The ones which are massively sent to entities in a much larger target audience – which can be easily detected;
2. Targeted emails which are crafted specifically for the receiving parties, sometimes even in their native language and correct information.

Mass Campaigns

Let’s take a look at the following non-targeted email:


From: Message Centre <3610sa@makerspacect.com>
Sent: Friday, September 13, 2019 12:39 PM
To: [redacted]
Subject: ResetPassword Friday, September 13, 2019

Office-365

Hi [redacted]

Due to request that you created ID: 3610
We need to confirm you as a owner of this email [redacted]
This validation valid until 13 September, 2019.

Confirm Ownership here for [redacted]

Thanks
mirosoft Corporation. All rights reserved. 2019 .

There are multiple key red flags in this email:

1. The “from” address is clearly fishy;
2. The message is poorly formatted and structured;
3. A deadline implies a sense of urgency to trick you into clicking the link as soon as possible;
4. Hovering over the link exposes a completely non-relevant domain:
   http://boutiquesque.com/cl/?
5. The footer references Microsoft which is misspelled and not relevant in this context;
6. No contact information is included.

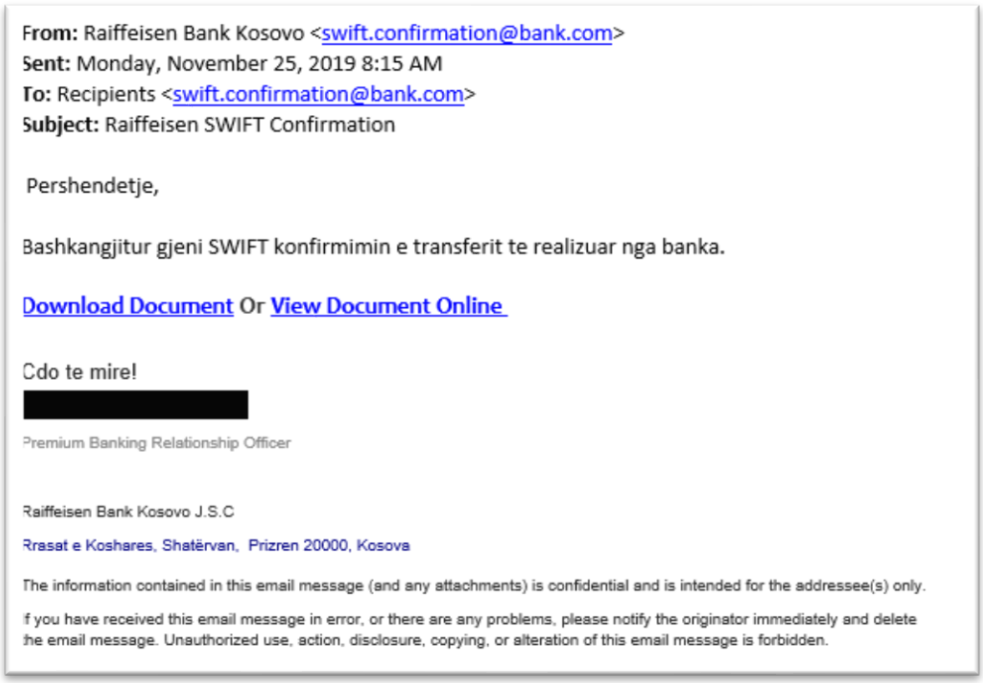
We recommend to simply ignore such cases and block the sender address or delete the message altogether.

Spear Phishing

Campaigns known as “spear phishing” are dangerous as they may look quite real even to tech-savvy people. Advanced attackers will impersonate entities after gathering as much information as they can. For instance, foreign actors will try to send emails in the native language of the receiver with attachments or links crafted to their profession or interests.

Unfortunately, the email protocol is not secure by design; attackers can send you emails from legitimate addresses of an entity (known as "email spoofing"). However, in these cases, reputable email providers such as Microsoft Outlook and Gmail will automatically detect and classify the vast majority of them as spam/junk. Hence, attackers try to avoid forged emails and instead use domains which are almost identical to the original one.

To best understand this technique, we will outline another case scenario which is typically used in a targeted manner appearing to be sent from our bank:



From: Raiffeisen Bank Kosovo <swift.confirmation@bank.com>
Sent: Monday, November 25, 2019 8:15 AM
To: Recipients <swift.confirmation@bank.com>
Subject: Raiffeisen SWIFT Confirmation

Pershendetje,

Bashkangjitur gjeni SWIFT konfirmimin e transferit te realizuar nga banka.

Download Document Or View Document Online

Cdo te mire!

[redacted]

Premium Banking Relationship Officer

Raiffeisen Bank Kosovo J.S.C

Rrasat e Koshares, Shatërvan, Prizren 20000, Kosova

The information contained in this email message (and any attachments) is confidential and is intended for the addressee(s) only.

If you have received this email message in error, or there are any problems, please notify the originator immediately and delete the email message. Unauthorized use, action, disclosure, copying, or alteration of this email message is forbidden.

At first sight, the email looks legitimate – it is in the native language of the client recipient, contains a signature which is similar to the one we use, and also uses the "*bank.com*" domain which may not be seen suspicious in the beginning, but in fact, it is; perhaps a good time for the reminder that we never use any other domain name except the official "*raiffeisen-kosovo.com*". Moreover, such emails are almost every time unexpected so you should be extra cautious before proceeding further.

As always, the best way to reach a conclusion is to hover onto the link(s) and pay attention to the domain that is referenced. If it does not match our official domain, then it is most likely fraudulent and should possibly be forwarded to siguria@raiffeisen-kosovo.com or to Customer Service at +383 (0)38 222 222.