The winning scam from Google: 'Game cat' for vigilant people, 'tragic' for those who are light-hearted

In computer security, there is no shortage of funny and bad situations, scams that seem to appear only in comedies.

When it comes to computer security, most of us think of serious cyberattacks, complex online fraudulent acts with the potential to cause financial loss, data loss and hardware damage, and may even make big businesses suffer. However, in computer security, there is no shortage of funny and bad situations, scams seem to appear only in comedies. Such as the case we are about to learn right now.

1. [Infographic] How to recognize and prevent Phishing attacks

Bonus scam

True story like kidding! Yes, this phishing campaign sent out a series of spam emails informing victims that Google will give them $ 2.5 million in bonuses as part of the gratitude program for loyal customers of the services. Google for many years.

Now is not the time to count on anyone being fooled after this ridiculous incident and send scammers their personal information (not much but I think it is), but a time to We further analyze these phishing scams and find out how to proactively identify the online fraudulent practices that are appearing on the internet every minute. ,

every second.

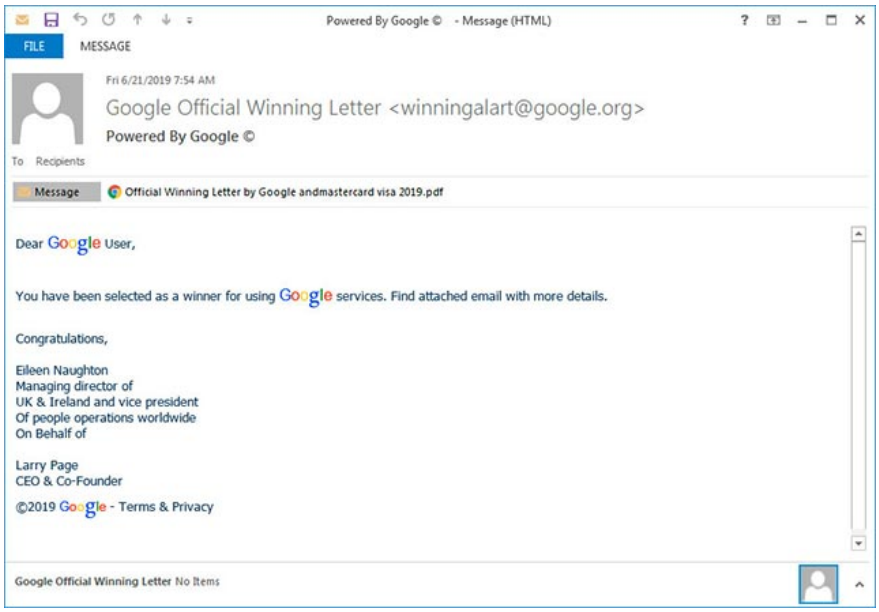
1. Hacker purged two-factor security just by automated phishing attacks

'Powered by Google'

This scam appears as an email with the subject line 'Powered by Google' as an affirmation of the level of credibility, saying "You have been selected as one of the loyal user prize winners. for Google services "(You have been selected a winner for using Google services).

To add legitimacy, crooks add additional lines of advertising that this email is being sent to you by a division manager, on behalf of Google CEO, Larry Page.

1. What is Whaling Attack? Why should CEOs pay special attention to this form of cyber attack?



"On behalf of CEO Larry Page"

Along with this phishing email is an attachment called "Official Winning Letter by Google and mastercard visa 2019.pdf." This attachment, as shown in the screenshot below, says you won. Awarded Google Visa / MasterCard (GVMC) with a total value of up to 2,500,000 USD!

In the next step the crook begins 'on the main issue' when asking the victim to fill out the required information correctly and return it to them to receive the prize. In the end, as we all know, no money will be transferred, while your extremely important personal information such as bank account information, credit cards, phone numbers and even even the account, the password has fallen into the wrong hands.

1. [Infographic] 4 types of Phishing are easy to trap users

Google Visa/MasterCard (GVMC) Award
Purchase Street, Purchase, NY 10577 United States.

Your e-mail address winning details:
- Award Batch No: GVMC/6736006529/2019
- E-Ticket No: 29700067360065291US
- E-Grant Amount: $2,500,000.00 USD

OFFICIAL WINNING NOTIFICATION LETTER

This is to inform you that you have been selected as a winner for using Google Services by the E-mail electronic online sweepstake organized by Google, in conjunction with the Foundation for the Promotion of Software Products (F.P.S.P) and confirmed by our co-sponsors Visa®/MasterCard® International. You have therefore awarded $2,500,000.00 USD with E-Ticket No: 29700067360065291US. Be informed that your prize has been insured and a Visa/MasterCard will be credited with the total sum won and delivered to your designated address which you are to provide to your claim administrator. We do believe with your prize, you will continue to be active in your usage of Google services and Visa/MasterCard products.

Furthermore, your winning prize delivery logistics will be superintended by our Afro-regional representative office as was indicated in your winning coupon slip. Your prize will be released to you upon meeting the requirement of the promotion award board authority which includes your statutory obligations. You are advised to contact our Foreign Payment Bureau with your Claims information as required below to file your Claims:

CLAIMS FORM
1) Full Names:
2) Address:
3) Phone Number:
4) Age:
5) Occupation:
6) Private Email Address:
7) Ever Won An Online Lottery?
8) How satisfied are you with Google? (A=Very Satisfied; B=Satisfied; C=Unsatisfied)

Send all response via email to our Foreign Payment Bureau officer below:

Name: David Yates
Designation: President, New Payment Platforms for Mastercard. Email: gwinnings01@googlemail.com

We value your right to privacy! Your information is 100% secured and will be used exclusively for the purpose of this award only.

NOTE!!! For security reasons, you are advised to keep your winning information confidential till your claims are processed and your money remitted to you. This is part of our precautionary measure to avoid double claiming and unwarranted abuse of this program. Please be WARNED!!!

Congratulations from the Staffs & Members of Google Visa/MasterCard (GVMC) Award International.

MD Ajay Banga,
President & CEO, Mastercard Int.

Larry Page
Co-Founder & CEO Google Inc.

Attachments of phishing emails

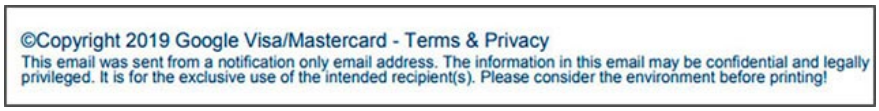
In particular there is a detail that we often encounter on most phishing emails in general, which is a warning to keep the information completely confidential. As in this case, crooks ask the victim to "keep the prize information confidential for security purposes and avoid other abuses." However, the real purpose of these requests is nothing super, simply not to let the victim reveal information to those who are more alert, leading to fraudulent practices being exposed. Therefore, this is also a common feature in every general fraudulent act that you should keep in mind.

1. How to protect yourself from phishing attacks via mobile phones

Keep the environment green - clean - beautiful

Looking down at the end of the phishing email, you will see a rather humorous information.

Specifically, at the end of the attachment, the scammer asks you "Please consider the environmental-related harm before deciding to print this email!" (Hãy Consider c? s? d? li?u tr??c khi printing!)



"Please consider the environmental-related harms before deciding to print this email!"

In fact, they don't care much about the environment, but the ultimate goal is to prevent victims from exposing this email to 'more alert' people, causing their fraudulent behavior to be discovered. But only, we are all nature lovers, consciously protecting a living school so I appreciate this practical 'proposal' of the scam group!

1. The 4 most popular types of network attacks towards older people

Response

Summarize the problem. It is possible that these types of winning scams are nothing new and relatively easy to catch, but it still deceives many people who lack security knowledge, are light-hearted. , and especially greed.

When you encounter emails of this type, there are 3 things you need to do. First, do not open the email attachments. Secondly, do not reply to emails as well as provide any information requested by a fraudster. And finally, ask the people around the candle to still feel "freaked out".

Wish you are always sober when you join this complicated Internet world!