Abertay University

Phishing – Be ready for attack

Phishing attacks methods and evaluation of defence strategies

Jacek Jajko

CMP320 : Ethical Hacking 3

BSc Ethical Hacking Year 3

2021/22

Note that Information contained in this document is for educational purposes.

.

Abstract

Phishing is a type of Internet attack that consists in impersonating another person or institution in order to obtain data, confidential information or to infect a computer. Some cases of phishing also involve actions aimed at getting the victim to perform particular actions, such as handing over money to criminals. Phishing is one of the simplest methods known to modern cybercrime, but at the same time it is still extremely virulent. The effectiveness of phishing stems from the fact that it uses soft mechanisms and the fact that humans are the weakest link in all security measures.

This document does not fully describe all available phishing attack and defence methods, only the ones chosen by the author. The following phishing related topics have been addressed in this document: process of creating phishing websites using open-source tool ‘HiddenEye’, homograph attack, identification of phishing websites using password manager, defence against phishing using U2F Security Key (demo of U2F configuration for Google account) and Passwordless login feature for Microsoft.

.

+Contents

.

1 INTRODUCTION

1.1 BACKGROUND

The term ‘phishing’ was coined in the mid-90s by crackers attempting to steal AOL accounts. The attacker impersonated an AOL employee and sent a message to a potential victim. The message requested a password, for example, to "verify your account" or "confirm the information in a bill." When the victim entered the password, the attacker gained access to the account and used it for illegal purposes, such as spamming (Ollmann, 2007).

Phishing is a prevalent sort of cybercrime that can be carried out using email, voice messaging, social networking sites, SMS-based services, or even multiplayer games. It employs social engineering, a strategy in which cyber criminals attempt to mislead you into acting in their favour. In the case of phishing, the attacker most often uses the authority of the person or institution he is impersonating, for example by contacting him as a supervisor, colleague, bank, electricity supplier, office, shipping company or a famous shop. The content of the message sent by the attacker is most often designed to elicit strong emotions in the recipient, such as fear, or to force the victim to act quickly, as the attacker anticipates (Chhikara, 2013).

Spear phishing is more sophisticated form of phishing that targets selected victims. Messages in this type of assault are personalised and make extensive use of previously gathered data about the victim. This might be data gathered by white intelligence and OSINT tactics, or it could be data received through leaks from other websites. With spear phishing, the victim receives a crafted e-mail or SMS message that makes it much harder for him to recognise at first glance that he is being targeted by a phishing attack (Bullée et al., 2017).

Cyber-attacks can affect many aspects of a company's business and incur different costs depending on the nature and severity of the incident. However, they are most often perceived through the prism of information that enterprises are obliged to disclose to the public, including, in particular, about the theft of personal data, health data or payment information. Incidents involving intellectual property theft, espionage, data destruction, attacks on core operations, or attempts to damage key infrastructure, on the other hand, are rarely discussed openly. Despite appearances, these types of attacks can have significantly more serious consequences for organisations and entail additional expenditures that firms not only cannot simply calculate, but also frequently fail to notify the public about (Mossburg, Gelinne and Calzada, 2016). The consequences of an attack can be disastrous for a company, regardless of its size. In 2021 phishing has been identified to be the second most common initial attack vector that on average cost the company $4.65 million (Ponemon Institute and IBM Security, 2021).

According to the Cisco "Cyber security threat trends: phishing, crypto top the list," phishing remains one of the most popular attacks, accounting for 90% of data breaches. Despite its age, it is still widely used due to its simplicity and effectiveness resulting from compromising the weakest link in the security chain: the user (Cisco, 2021). Research conducted by Tessian (cloud email security platform that prevents advanced email threats) found that employees received on average 14 malicious email messages in 2021. Certain businesses were more vulnerable to phishing, for example, retail employees got an average of 49 such messages (Rosenthal, 2022).

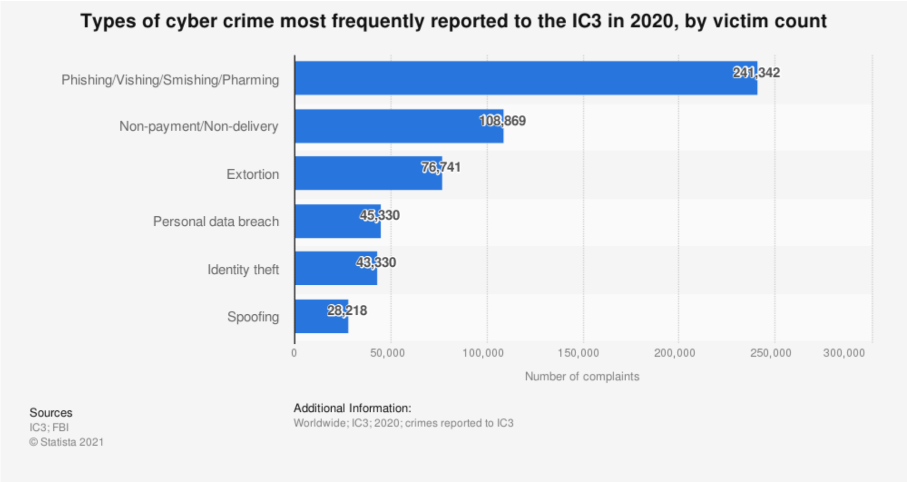


Figure 1 Types of cybercrime most frequently reported to the IC3 in 2020, by victim count

1.2 AIM

Protecting against phishing can be quite a challenge for an average user. Recognising phishing is not always easy, but with a few tips, some discipline and common sense, you can avoid the threat.

The aim of this project is to conduct research and describe findings in the following phishing attacks topics:

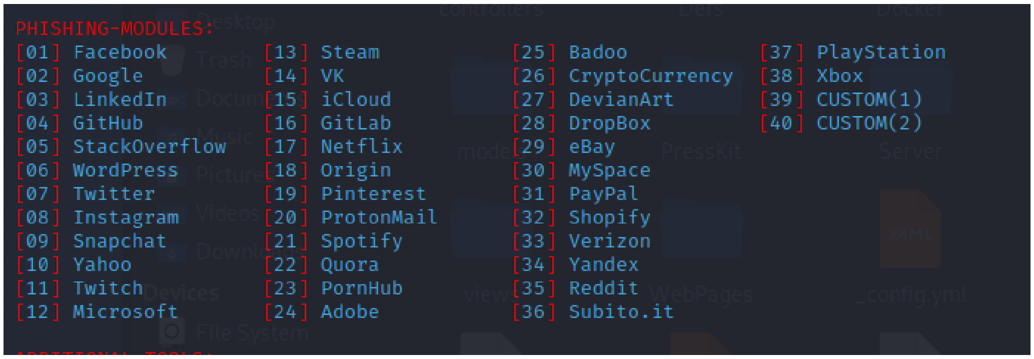
- Creation of a phishing website using the HiddenEye,
- Homograph attack
- Registration of domains with foreign characters
- How phishing website can be identified using a password manager
- Origin binding: defence against phishing using U2F Security Key

The purpose of this report is to bring the subject of phishing closer to the reader and to demonstrate effective methods of protection against them.

2 PROCEDURE

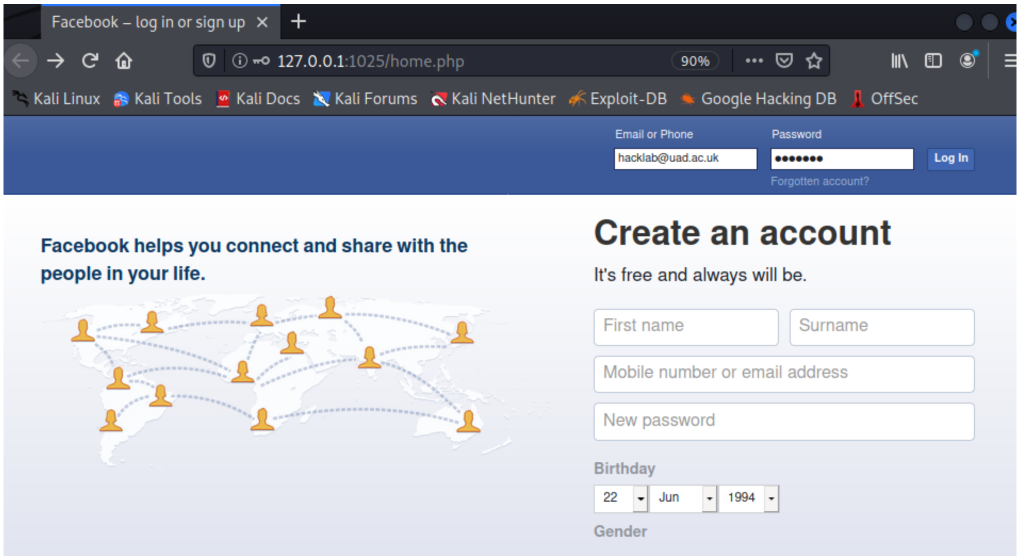
2.1 HIDDENEYE - MODERN PHISHING TOOL

HiddenEye is a sophisticated phishing tool with advanced capabilities shared on GitHub by the user 'Morsmalleo'. Despite the fact that the creators of this program clearly specified its use for educational purposes only, it can be used by hackers to launch a phishing attack. It not only supports the creation of phishing websites but also allows the user to carry out a variety of phishing attacks. There are numerous 'phishing-modules' which acts as a ready to deploy template for a phishing website (Figure 2). We created a phishing 'Facebook' website to show how believably HiddenEye can reflect the real website (Figure 3).



```
PHISHING-MODULES:
[01] Facebook        [13] Steam          [25] Badoo           [37] PlayStation
[02] Google          [14] VK             [26] CryptoCurrency  [38] Xbox
[03] LinkedIn        [15] iCloud         [27] DevianArt       [39] CUSTOM(1)
[04] GitHub          [16] GitLab         [28] DropBox         [40] CUSTOM(2)
[05] StackOverflow   [17] Netflix        [29] eBay
[06] WordPress       [18] Origin         [30] MySpace
[07] Twitter         [19] Pinterest      [31] PayPal
[08] Instagram       [20] ProtonMail     [32] Shopify
[09] Snapchat        [21] Spotify        [33] Verizon
[10] Yahoo           [22] Quora          [34] Yandex
[11] Twitch          [23] PornHub        [35] Reddit
[12] Microsoft       [24] Adobe          [36] Subito.it
```

Figure 2 Phishing modules included in HiddenEye



Email or Phone: hacklab@uad.ac.uk
Password: •••••••
Log In
Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

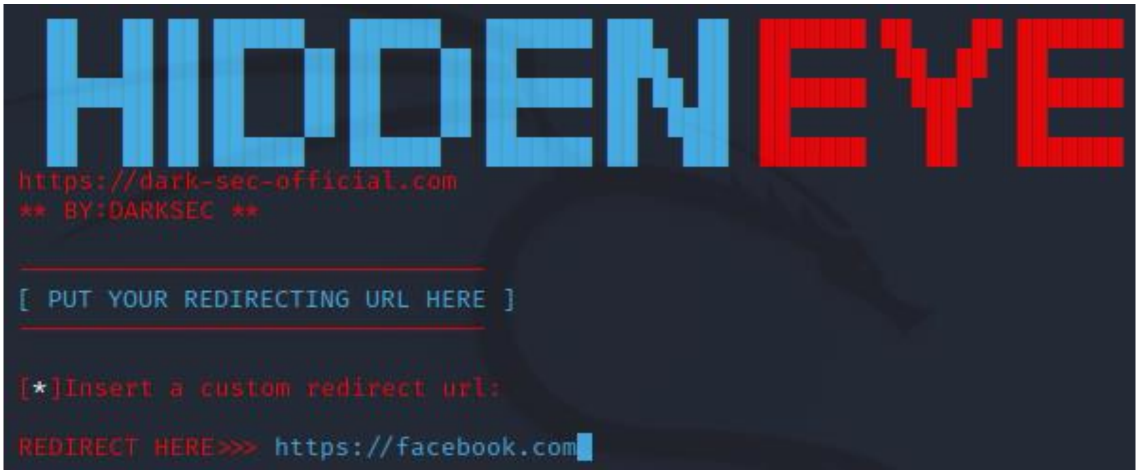
First name | Surname
Mobile number or email address
New password

Birthday
22 | Jun | 1994

Gender

Figure 3 Example of a phishing 'Facebook' website

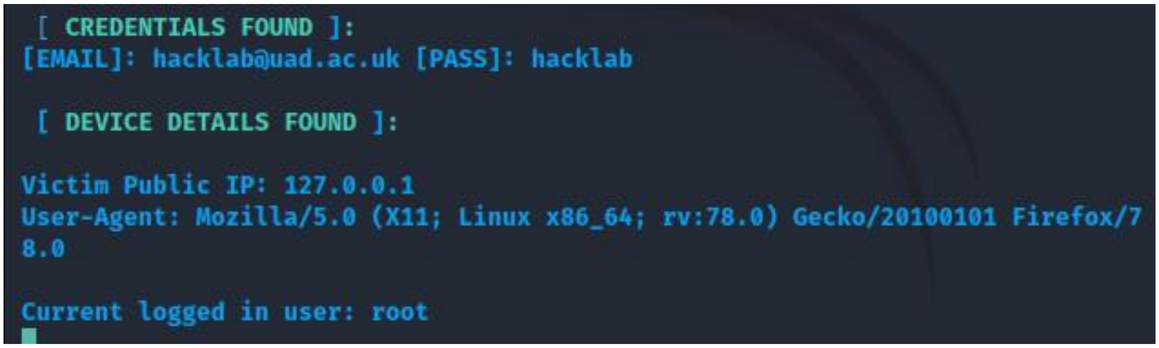
HiddenEye configuration requires providing a redirect URL(Figure 4). It will be used to forward the victim to the website of our choice i.e. a phishing ‘Facebook’ website can be created and when the user presses the ‘Login’ button he will be redirected to the original Facebook page. If our victim was previously logged in to Facebook on the browser from which he clicked on the link to our phishing site, he may not realise he is a victim of phishing because he will see his account to which he is logged in. Otherwise, he may be slightly surprised as he has not logged on to the site.



```
HIDDENEYE
https://dark-sec-official.com
** BY:DARKSEC **

[ PUT YOUR REDIRECTING URL HERE ]

[*]Insert a custom redirect url:

REDIRECT HERE>>> https://facebook.com
```

Figure 4 HiddenEye configuration - Redirect URL

If our victim opens and logs in to our phishing site, we gain a lot of useful information: credentials, IP address, web browser and current logged in user (Figure 5).



```
 [ CREDENTIALS FOUND ]:
[EMAIL]: hacklab@uad.ac.uk [PASS]: hacklab

 [ DEVICE DETAILS FOUND ]:

Victim Public IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/7
8.0

Current logged in user: root
```

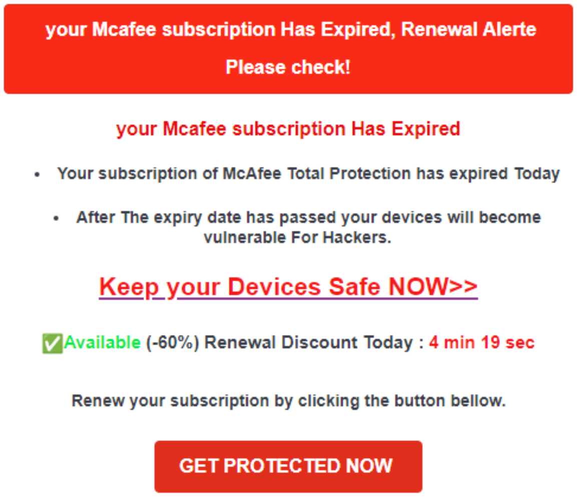
Figure 5 HiddenEye victim's details

2.2 RECOGNITION OF PHISHING EMAILS

Until you are sure that the sender is genuine, you should not click on or reply to any links. SMS and e-mail messages often use shortened website addresses. Therefore, it is recommended that you pay special attention to the names of websites that are sent in suspicious emails or SMS messages, e.g., a fake http://login-fb.com/ address may be used instead of https://www.facebook.com. The next thing is to determine if the email is genuine and not a scam (Figure 6).

How to recognize a phishing email?

- Many phishing messages have incorrect grammar, punctuation, or spelling.
- Check if the email is addressed to you by name, does it refer to a 'valued customer', 'friend' or 'colleague'? This could mean that the sender does not really know you and that it is part of a phishing scam.
- Beware of shortened links, if you are unsure where a link will take you, use a website like https://www.checkshorturl.com/ that can check the link for you.
- Pay attention to links passed between friends, check if the link actually leads to the correct page. It is becoming increasingly common for criminals to illegally gain control over our social media accounts by impersonating our friends and family.
- Check if the email contains a hidden threat that requires immediate action? Be suspicious of words like "send this data within 24 hours" or "you are a victim of crime, click here immediately".



your Mcafee subscription Has Expired, Renewal Alerte
Please check!

your Mcafee subscription Has Expired

- Your subscription of McAfee Total Protection has expired Today
- After The expiry date has passed your devices will become vulnerable For Hackers.

Keep your Devices Safe NOW>>

✅Available (-60%) Renewal Discount Today : 4 min 19 sec

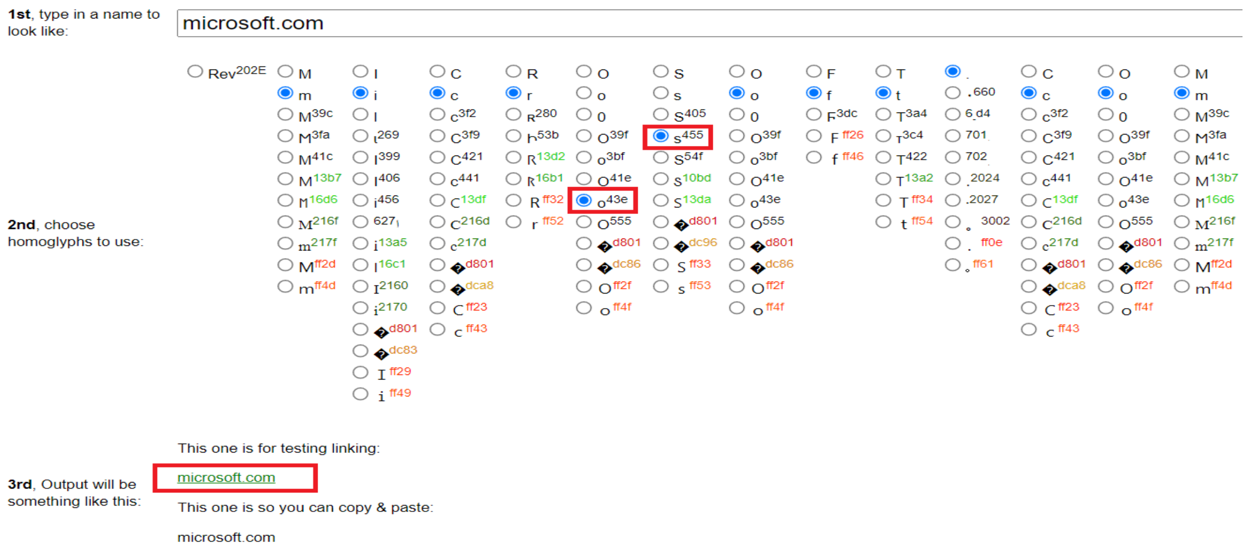
Renew your subscription by clicking the button bellow.

Figure 6 Example of phishing email

If you notice a suspicious email, mark it in your inbox as spam or junk or suspicious. This will remove it from your inbox and inform your email provider that you have identified it as potentially dangerous.

2.3 HOMOGRAPH ATTACK

The homographic attack is based on modern Internet standards that allow the creation (and display in browsers) of URLs containing characters from non-Latin (i.e. non-ASCII) alphabets. Different alphabets can contain different characters that are very similar to each other. Attackers can therefore register their own domains, confusingly similar to existing Internet addresses. This attack was first described by Alex Gontmakher and Evgeniy Gabrilovich, who conducted a feasibility study of this type of attack on the microsoft.com domain (Gabrilovich and Gontmakher, 2002). They managed to register a homographic domain name “http://www.microsoft.com“ containing Russian letters ‘c’ and ‘o’(Figure 7).



1st, type in a name to look like: microsoft.com

2nd, choose homoglyphs to use:

3rd, Output will be something like this:

This one is for testing linking:

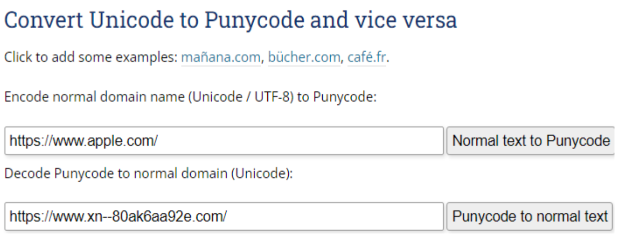
microsoft.com

This one is so you can copy & paste:

microsoft.com

Figure 7 Visualization of the attack using Homoglyph Attack Generator (https://www.irongeek.com/homoglyph-attack-generator.php)

In 2017 a Chinese information security researcher Xudong Zhenghas presented a "nearly impossible to detect" phishing attack that can fool even the most cautious Internet users. Using Punycode (encoding syntax that converts a Unicode (UTF-8) string of characters into the ASCII characters allowed in host names)(Costello, 2003), he managed to register an ‘apple.com’ look-alike domain(Figure 8)(Figure 9).



Convert Unicode to Punycode and vice versa

Click to add some examples: mañana.com, bücher.com, café.fr.

Encode normal domain name (Unicode / UTF-8) to Punycode:

https://www.apple.com/ | Normal text to Punycode

Decode Punycode to normal domain (Unicode):

https://www.xn--80ak6aa92e.com/ | Punycode to normal text

Figure 8 Conversion from Unicode to Punycode

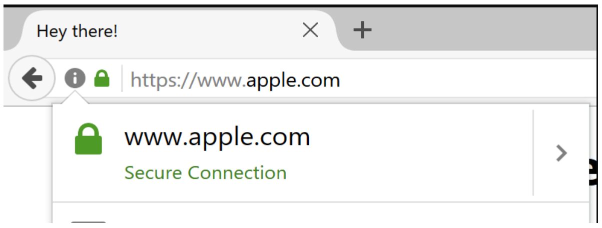


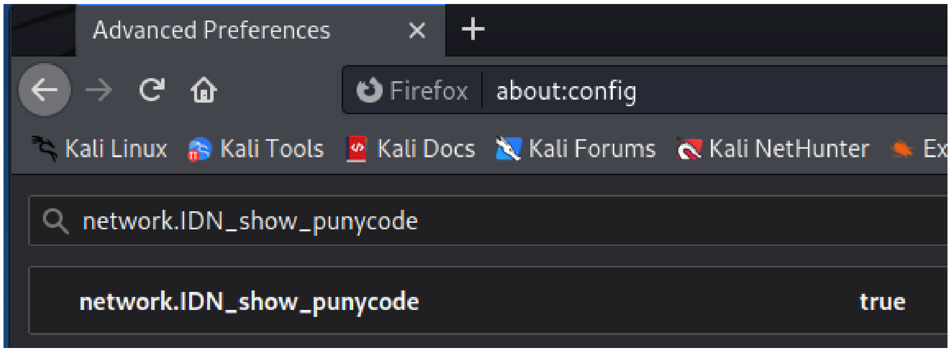
Figure 9 'apple.com' domain registered by Xudong Zhenghas (https://www.xudongz.com/blog/2017/idn-phishing/)

Because of the increased frequency of homographic attacks, Google has implemented modifications to the web browser to better protect users from bogus websites and attacks. They have been introduced in Chrome Stable 58 version (Lynch, 2017).

To avoid homograph attacks, users of various browsers can apply the following strategies:

- disabling the Punycode service in web browsers
- not accessing websites whose links appear in incoming e-mails
- not visiting websites that look suspicious

Firefox users can independently make the deactivation of Punycode encoding conversion. They have to type **about: config** in the address bar and then hit enter. The next step is to set the **network.IDN_show_punycode** parameter to **True (**Figure 10**)**.



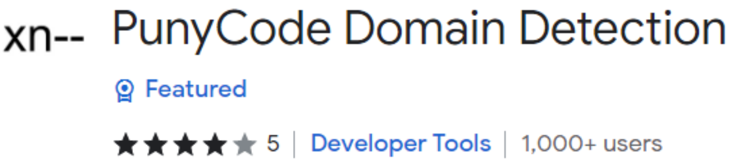
about:config

network.IDN_show_punycode

network.IDN_show_punycode **true**

Figure 10 Firefox show_punycode option

This leads to the fact that all domains which have letters and characters other than those of the Latin alphabet are displayed as Punycode. Chrome or Opera browsers do not offer this option, however, in the case of the Google browser, it is possible to use external extensions (Figure 11) .



PunyCode Domain Detection

Featured

★★★★☆ 5 | Developer Tools | 1,000+ users

Figure 11 Chrome Web Store Punycode Domain Detector

2.4 DETECTION OF PHISHING WEBSITES USING PASSWORD MANAGERS

A password manager's primary function is to securely store data in a single location. It acts as a "vault" in its assumptions, where you may store your most essential passwords and data for automated filling, such as addresses, payment cards, and many others. Surprisingly it can also be used to detect phishing websites (LastPass, 2019). Using the LastPass password manager as an example, this section will show how a user can check if a page they have opened is genuine .

From the previous chapters, we learned that cybercriminals create fraudulent websites and offers that look similar to legitimate ones in order to deceive users who mistype the URL or are not paying close attention. This risk is mitigated by the LastPass extension, which automatically navigates to the trusted webpage because the URL is already saved in the vault. LastPass stores only login information for sites that user saved in the vault so whenever a phishing website is opened, that looks very similar to the genuine website, LastPass will not show the autofill option, because it does not recognize the website (LastPass, 2019).

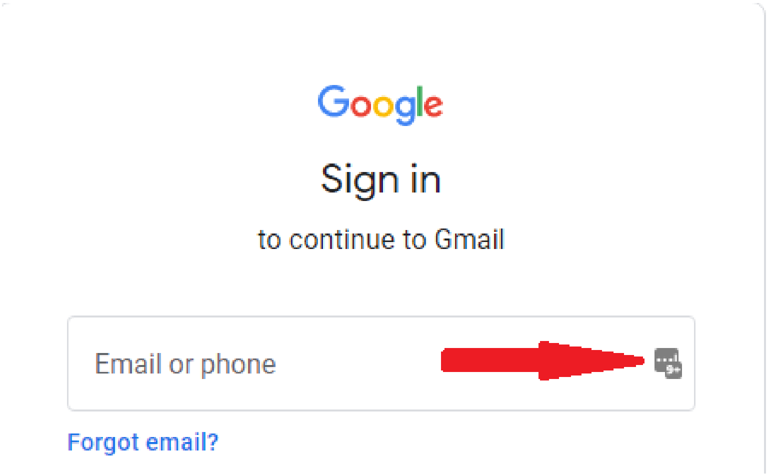


Figure 12 LastPass autofill icon

LastPass can be used free of charge for private use. For companies, LastPass business licences is available. It extends the functions of the password manager by offering additional security. These include:

- multi-factor authentication,
- biometric authentication,
- shared password folders,
- monitoring the dark web for broken addresses/logins,
- security reporting.

2.5 DEFENCE AGAINST PHISHING USING U2F SECURITY KEY

A password is the easiest way to prove who we are when we want to log in to Internet services. Unfortunately, more and more often passwords cease to be a good security measure. Even if we use special characters and lowercase and uppercase letters in the process of creating an account, we cannot be sure that it will not be broken. Therefore, it is recommended to use a two-step verification. This method involves double-checking your identity when logging in. Stage one requires you to enter your login and password in the login panel. At stage two, in order to log in, you must provide a second component, such as : a code sent in an SMS message, or a code generated in a mobile application (such as Google Authenticator) or a U2F security key.

The accessories called U2F keys are gadgets that look like memory sticks (Figure 13), but their design is much more complicated. Their purpose is to provide the highest level of security, which is not provided by codes sent via SMS (the SIM card can be cloned) and via e-mail (mail can be hacked, both on the client and server side). Multi-level authentication using U2F (Universal 2 Factor) keys has a similar principle, but the whole process is slightly different. The core of this method is the so-called physical token, i.e., a small device that has to be plugged into a USB port on the computer at the time of logging in. An additional confirmation is secret data encrypted in its memory. The U2F key is the only two-step authentication method that completely protects against the effects of phishing. Even if you are fooled by a cybercriminal and enter your username and password on a fake website, if you use the U2F key for two-step authentication, the attacker will not be able to take over your account.

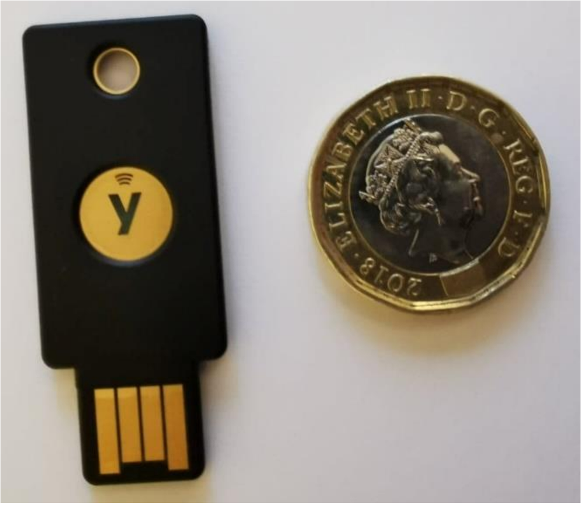


Figure 13 Yubico - YubiKey 5

Pros of U2F:

- it does not require installation, configuration, or power supply
- it is small and handy and does not require power (you can carry it with your keys)
- one key can protect any number of accounts on any number of services and can be used on any number of devices (computers, smartphones, tablets, etc.)
- is the only method that protects against phishing in 100%

Cons of U2F:

- requires the purchase of a key

Although one key can be configured for multiple sites, it is recommended that two keys be purchased and configured for each site that allows it. The owner of the keys should designate one of them as the "primary key" and keep it with him. The secondary key should be kept in a secure location and used only if the primary key is lost. The disadvantage of using a U2F key is that not all online services support them, but the most popular portals such as: Facebook, Twitter and Google have taken care of this. Another disadvantage is a fact that the user has to enter login and password every time they login. The solution to this issue is FIDO2 security key, which allows the user to log in using the key and short PIN (instead of login and password).

YubiKey 5 series is a multi-protocol security key that supports: FIDO2, U2F, Smart Card ,OTP and OpenPGP3 protocols. It supports multiple popular applications. When you try to log in, YubiKey decrypts the query containing the previously generated key. The whole point is to touch the golden circle to activate the token at a given time. It is not enough to just insert the token in the USB. Every time user wants to use it, he has to touch it. The LED will light up and the authentication process will be performed. In the case of logging in to a page with U2F, you will be taken to the desired content after tapping it. YubiKey has other functions hidden under the magic button. It has two slots for holding passwords. If user holds finger down for about a second, the password from slot one will be pasted. If he does this for three seconds the password from the second slot will be pasted. It does not store any other information about the user, so even if it is lost no one will know where to use it (yubico, n.d.).

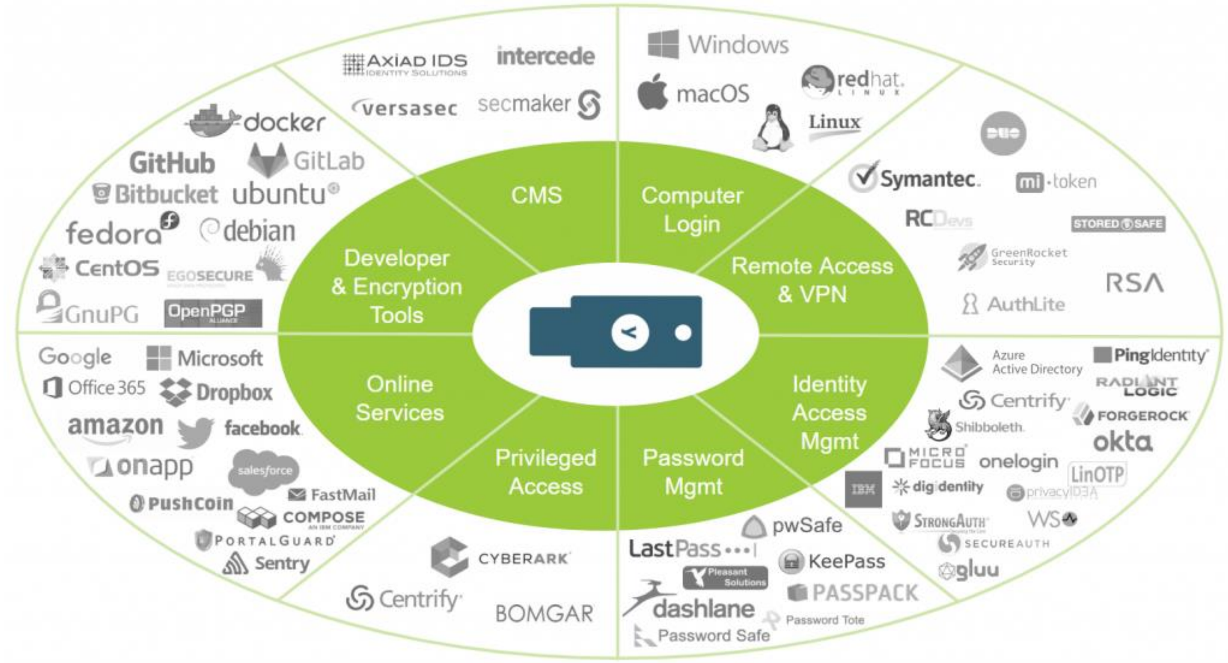
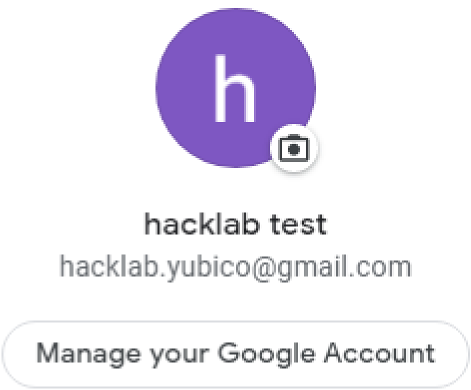


Figure 14 Applications supporting YubiKey source: https://www.yubico.com/

2.6 Using YubiKey To Configure U2F On The Gmail Example

Users can use security keys for 2-Step Verification to help protect their Google Accounts from hackers. In this paragraph, we discuss the configuration of U2F on the Gmail e-mail service. The first step is the purchase of the security key. There are many options available on the market but in this example, we used YubiKey 5 purchased on Amazon for £46.99. As a user, you should consider whether the security of your email is more valuable than the cost of the YubiKey or other security key of your choice.

To set up the U2F, open your Gmail and click on 'Manage your Google Account' (Figure 15).

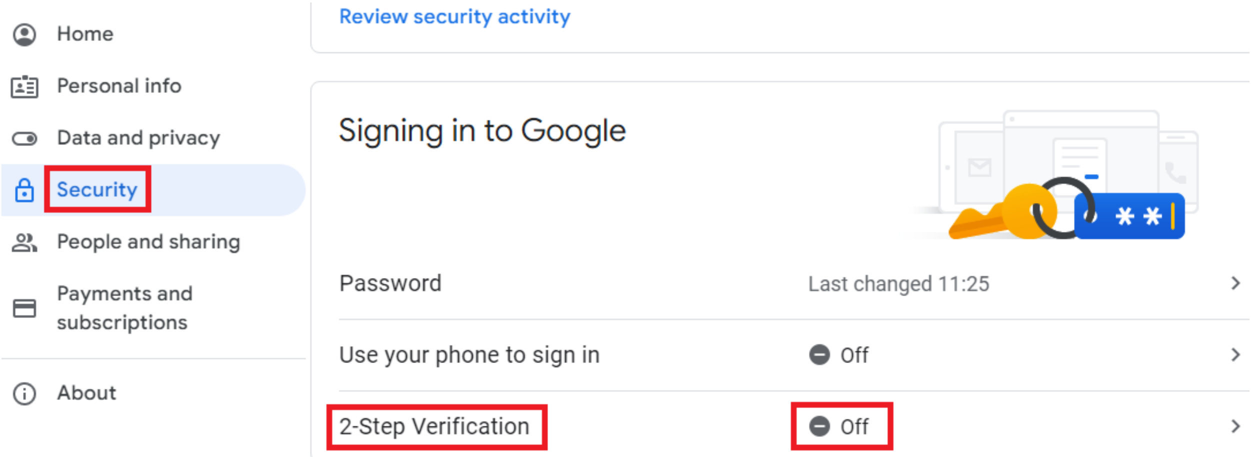


hacklab test

hacklab.yubico@gmail.com

Figure 15 Gmail Account window

Head into the '**Security**' tab, the '**Signing into Google**' should appear displaying available login options. We are interested in 2-Step Verification (Figure 16), click on it.



Signing in to Google

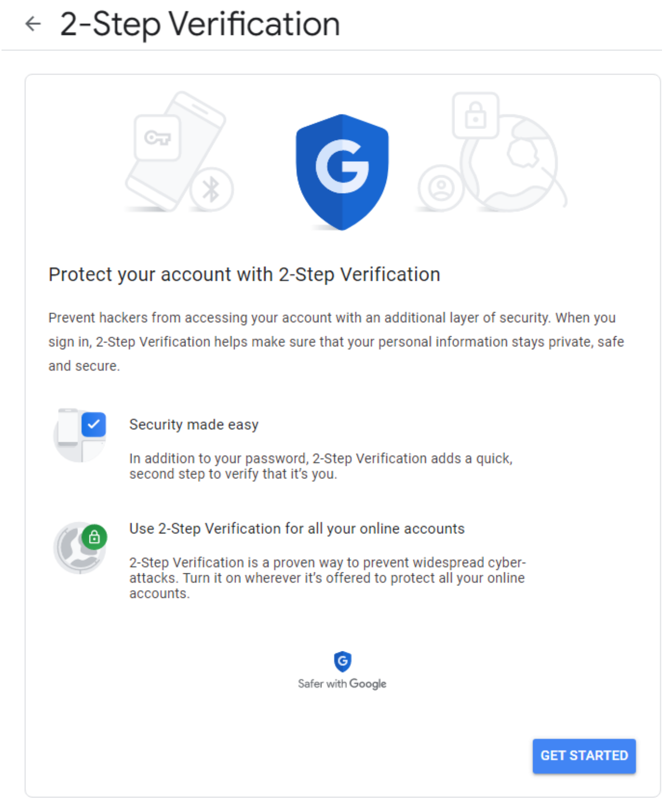
Password Last changed 11:25

Use your phone to sign in Off

2-Step Verification Off

Figure 16 Gmail Security tab

You should be redirected to the “2-Step Verification” window. Click ‘**Get Started**’, and from here, the process of U2F configuration begins (Figure 17).



2-Step Verification

Protect your account with 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security. When you sign in, 2-Step Verification helps make sure that your personal information stays private, safe and secure.

Security made easy

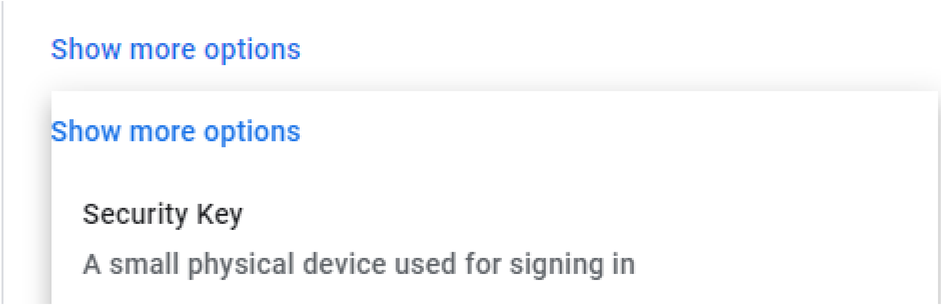
In addition to your password, 2-Step Verification adds a quick, second step to verify that it's you.

Use 2-Step Verification for all your online accounts

2-Step Verification is a proven way to prevent widespread cyber-attacks. Turn it on wherever it's offered to protect all your online accounts.

Figure 17 2-Step Verification Configurator

Look for the ‘**Show more options**’ button and select the ‘**Security Key**’ option (Figure 18).

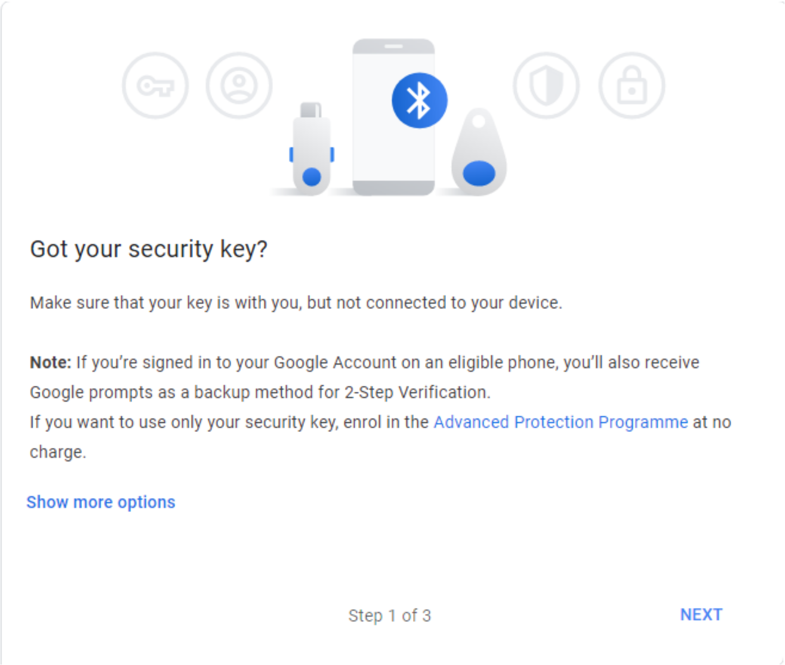


Security Key

A small physical device used for signing in

Figure 18 Show more options window

We are almost there, please read carefully all the information in the configuration process. This will help you to understand the procedure and will allow you to perform it in the future on your own. Press ‘Next’ in this step (Figure 19).



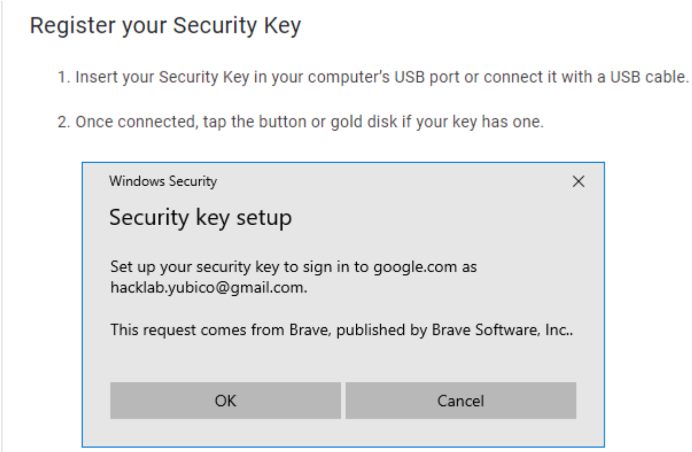
Got your security key?

Make sure that your key is with you, but not connected to your device.

Note: If you’re signed in to your Google Account on an eligible phone, you’ll also receive Google prompts as a backup method for 2-Step Verification.
If you want to use only your security key, enrol in the Advanced Protection Programme at no charge.

Figure 19 2-Step Configuration Process

Now, you have to insert the YubiKey into USB port (Figure 20) and touch the metal plate with ‘y’ logo (Figure 21).



Register your Security Key

1. Insert your Security Key in your computer’s USB port or connect it with a USB cable.
2. Once connected, tap the button or gold disk if your key has one.

Windows Security

Security key setup

Set up your security key to sign in to google.com as hacklab.yubico@gmail.com.

This request comes from Brave, published by Brave Software, Inc..

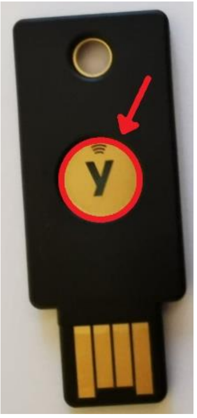
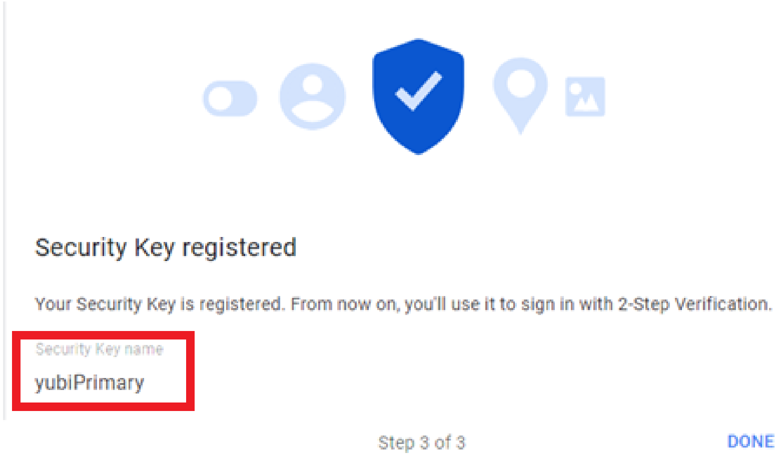


Figure 20 Registering the Security Key

Figure 21 YubiKey gold disc button

Once the security key has been registered, you should see the confirmation. It is required to provide a name for the security key (Figure 22) .



Security Key registered

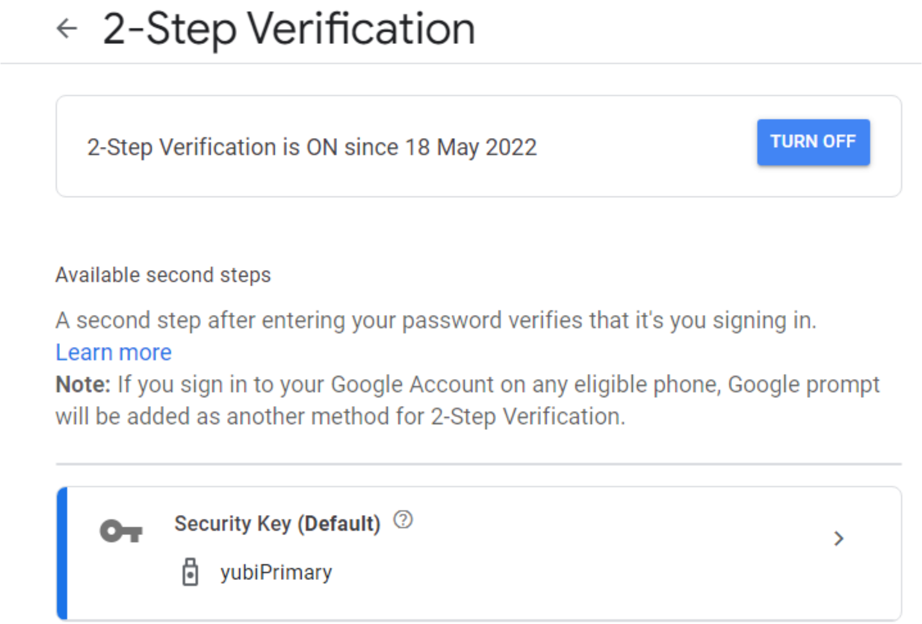
Your Security Key is registered. From now on, you'll use it to sign in with 2-Step Verification.

Security Key name

yubiPrimary

Figure 22 Security key registered

To check if the security key has been configured, open the ‘Security’ tab in Gmail (Figure 23).



2-Step Verification

2-Step Verification is ON since 18 May 2022

Available second steps

A second step after entering your password verifies that it's you signing in.
Learn more

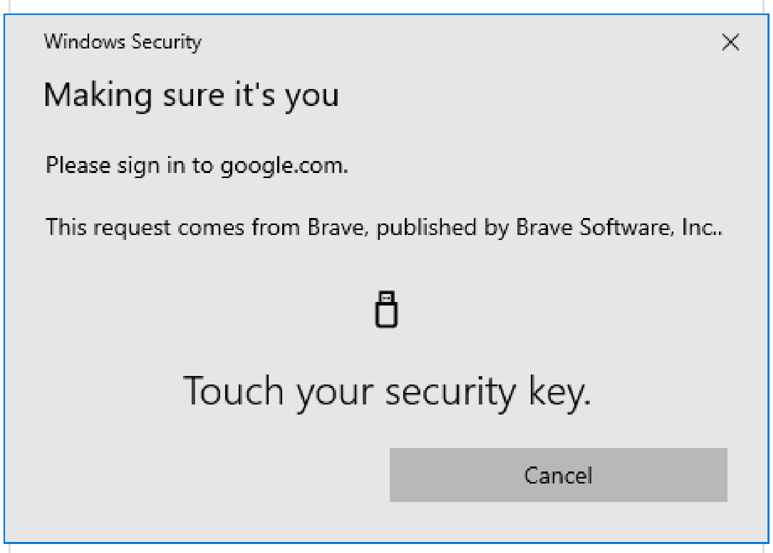
Note: If you sign in to your Google Account on any eligible phone, Google prompt will be added as another method for 2-Step Verification.

Security Key (Default)

yubiPrimary

Figure 23 2-Step Verification is Security tab

Now, every time after providing username and password, user will be asked to touch the security key in order to log in (Figure 24).


Windows Security

Making sure it's you

Please sign in to google.com.

This request comes from Brave, published by Brave Software, Inc..

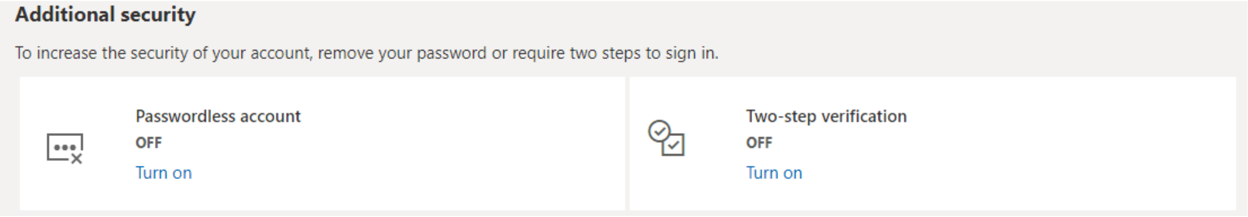
Touch your security key.

Figure 24 2-Step Verification asking user to touch the key

2.7 Passwordless Login With Microsoft Accounts & YubiKey

FIDO2 security keys can be used to sign into Azure AD or Azure AD Windows 10 hybrid joined devices and get single sign-on to cloud and on-premises resources. In 2021 Microsoft announced that their users can completely remove the password from their account and use Passwordless account option. In Microsoft's assumptions, one's own face and an application should suffice for logging in. Microsoft Authenticator for smartphone and Windows Hello have been introduced for this purpose, while a code sent to the phone number provided will be used for authentication. All in all, this is not new since 2017, but before the debut of Windows 11, Microsoft begins to heavily promote the "world without passwords" (Microsoft, 2022). Another option to assess Passwordless feature are FIDO2 security keys. They are a great solution for enterprises that are very sensitive to security or have scenarios or employees who are not ready or may use the phone as a second authentication factor.

To configure Passwordless on Microsoft account, it is required to setup the Microsoft Authenticator at first in ‘Additional security’ settings . The user is required to download the 'Microsoft Authenticator' application and perform the configuration.


Additional security

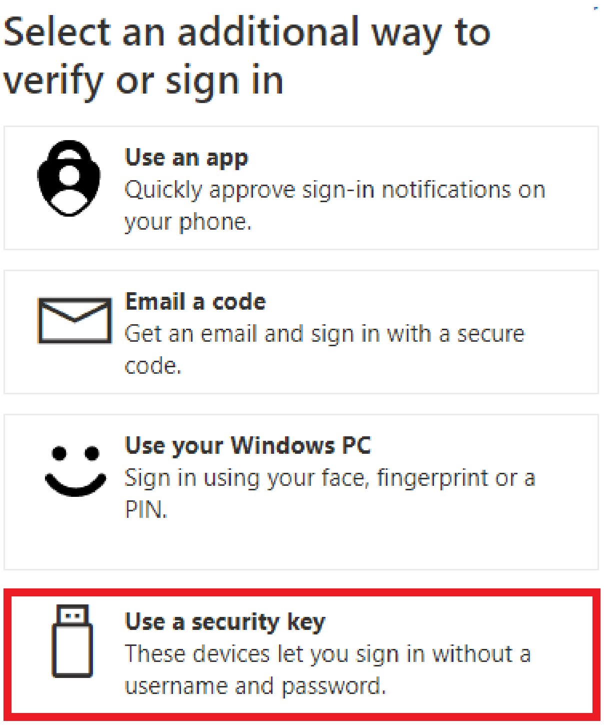
To increase the security of your account, remove your password or require two steps to sign in.

Passwordless account
OFF

Two-step verification
OFF

Figure 25 Microsoft Additional Account Security Menu

Now, it is possible to configure an additional way for the user to sign in. We would like to login without username and password using a security key (Figure 26). The configuration process is very simple and very well described (Figure 27).



Select an additional way to verify or sign in

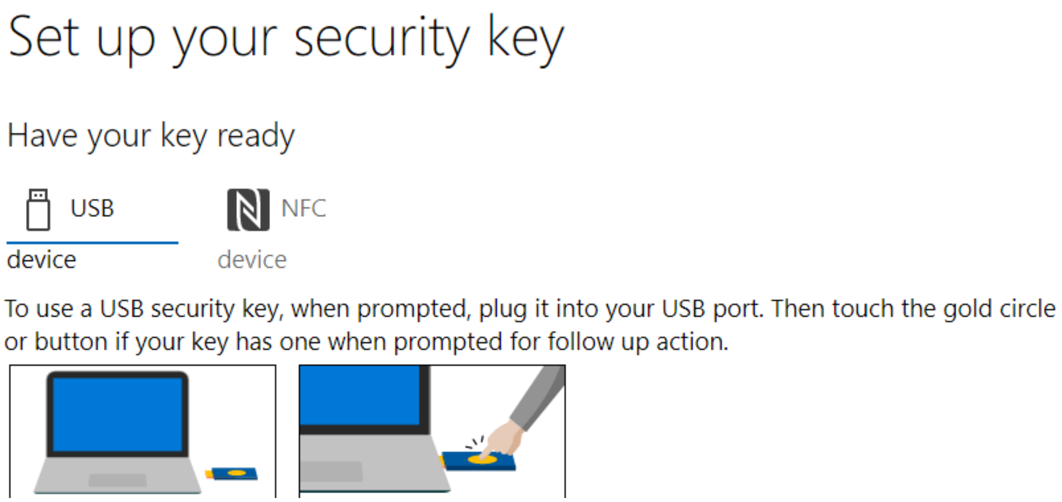
Use an app
Quickly approve sign-in notifications on your phone.

Email a code
Get an email and sign in with a secure code.

Use your Windows PC
Sign in using your face, fingerprint or a PIN.

Use a security key
These devices let you sign in without a username and password.

Figure 26 Additional ways to sign into Microsoft Account



Set up your security key

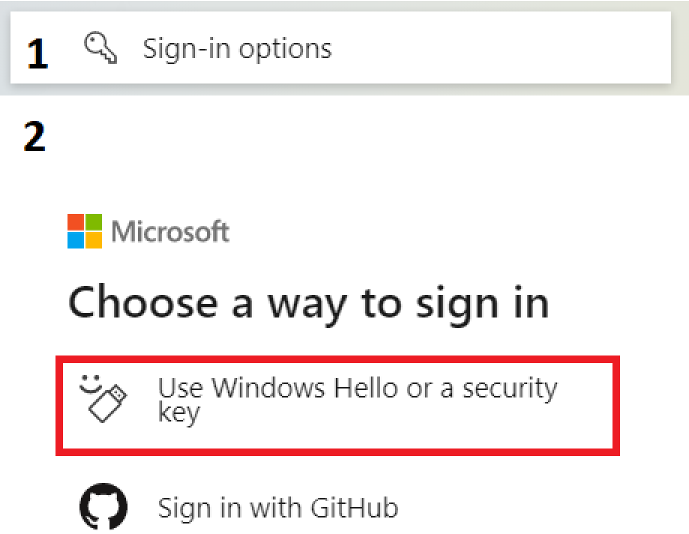
Have your key ready

USB device | NFC device

To use a USB security key, when prompted, plug it into your USB port. Then touch the gold circle or button if your key has one when prompted for follow up action.

Figure 27 Security key setup

To log in to your Microsoft account, select ‘Sign-in options’ and then ‘Use Windows Hello or a security key’ (Figure 28).



Sign-in options

Microsoft

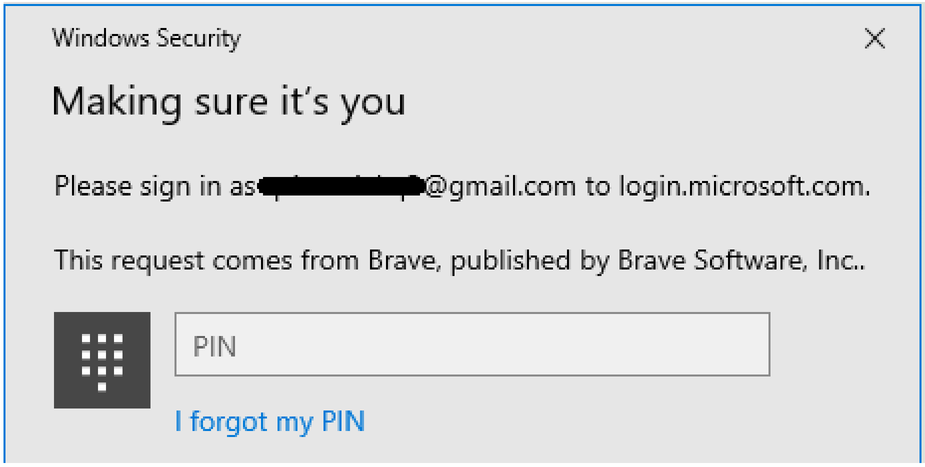
Choose a way to sign in

Use Windows Hello or a security key

Sign in with GitHub

Figure 28 Sign-in process

Remember to have the security key inserted into the USB port. You will be asked to provide a PIN that you set up during the Passwordless feature configuration. From now, to login into your Microsoft account you will only need a PIN and of course the security key.



Windows Security

Making sure it’s you

Please sign in as [redacted]@gmail.com to login.microsoft.com.

This request comes from Brave, published by Brave Software, Inc..

PIN

I forgot my PIN

Figure 29 Request for PIN during Passwordless login to Microsoft Account

3 DISCUSSION

3.1 GENERAL DISCUSSION

Account passwords can be unreliable. Short ones are easy to guess, while long ones can be difficult to remember. On the other hand, if you write them down somewhere, there is a risk that they will fall into someone's hands. Therefore, it is safer to use a simple password supported by two-factor verification.

When is it worth using multi-factor authentication? It is best to do it whenever a given service offers it, and we think that the data stored in our account is valuable and we would not like it to fall into hands of third parties. This may include your Gmail account. It certainly contains important messages from contractors, customer data, confidential information, or documents that, if in the hands of unauthorised persons, could harm the interests of our company.

The main issue when it comes to phishing protection is for users to be cautious. Employees should be aware of the risks associated with:

- opening links in emails,
- opening attachments in emails,
- accessing suspicious websites.

For this purpose, it is worth organising training on phishing in the company. So that employees know what to do when they receive a suspicious message. So that they do not click thoughtlessly on links they receive in e-mails. Employees should have it ingrained in their heads that before clicking on anything, it is worth thinking twice beforehand whether it is not a "trap". Good employee habits will certainly help to protect your company from losing important information.

In 2017, Google made it a requirement for its employees to use security keys at work. The goal of such a decision was to boost the security of sent business messages and documents. This method proved to be a success. After changing the security rules, none of the American company's 85,000 employees were victims of online fraud involving phishing and interception of company correspondence (Burgess, 2018). Google values the security of its users highly, which is why they introduced the“ Advanced Protection Program ”. The programme is aimed at journalists, activists, and entrepreneurs, among others, but it is safe to recommend to anyone who is paranoid. Participation in the programme necessitates the purchase of two security keys, as SMS codes or the Google Authenticator application are not supported (Google, n.d.).

Despite the numerous advantages of security keys, it should be remembered that they are not a substitute for logical thinking. While the YubiKey makes phishing attacks much more difficult, phishing is a social engineering attack. In other words, we trick the victim into providing us with their credentials. So, if the offender is aware that the user is using a dongle, he may try to trick him into downloading malware. It is true that interaction on the part of the equipment owner is required (logging in and inserting the key into the USB port), but for a properly determined attacker, this state of affairs will not be a major problem.

3.2 CONCLUSIONS

There are multiple ways of defending you or your company against phishing attacks. It can be achieved through staff awareness trainings. Employees must be aware of different phishing patterns and be able to recognize suspicious emails. Hardware keys, such as YubiKey, can easily and quickly help protect your account against phishing. At the same time, it is worth bearing in mind that hardware keys are not a cure for all "cyber problems" - an attacker may trick us into downloading and run malware that will be a kind of gate for the criminal to our confidential data.

As a business, you should consider using 2-Step verification solutions to further secure your account. It is worthwhile to use two-step verification to avoid data theft, which has numerous negative consequences. Effective defence against phishing can be also achieved by using a password manager. It is a free solution offering reliable protection that uses the autofill feature only on the exact website on which user saved their credentials on.

REFERENCES

Bullée, J.-W., Montoya, L., Junger, M. and Hartel, P. (2017). *(PDF) Spear phishing in organisations explained*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/320207541_Spear_phishing_in_organisations_explained.

Burgess, R. (2018). *Google's introduction of Security Keys for its staff killed employee phishing | KitGuru*. [online] kitguru.ne. Available at: https://www.kitguru.net/peripherals/pen-drives/ryan-burgess/googles-introduction-of-security-keys-for-its-staff-killed-employee-phishing/ [Accessed 18 May 2022].

Chhikara, J. (2013). *Phishing & Anti-Phishing Techniques: Case Study*. [online] *www.researchgate.net*. Available at: https://www.researchgate.net/publication/263773425_Phishing_Anti-Phishing_Techniques_Case_Study [Accessed 12 May 2022].

Cisco (2021). *Cyber security threat trends: phishing, crypto top the list*. [online] *umbrella.cisco.com*. Available at: https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list [Accessed 12 May 2022].

Costello, A. (2003). *RFC 3492 - Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)*. [online] datatracker.ietf.org. Available at: https://datatracker.ietf.org/doc/html/rfc3492 [Accessed 12 May 2022].

Gabrilovich, E. and Gontmakher, A. (2002). The homograph attack. *Communications of the ACM*, 45(2), p.128. doi:10.1145/503124.503156.

Google (n.d.). *Google Advanced Protection Program*. [online] Google Advanced Protection Program. Available at: https://landing.google.com/advancedprotection/ [Accessed 20 May 2022].

LastPass (2019). *#1 Password Manager & Vault App, Enterprise SSO & MFA | LastPass*. [online] Lastpass.com. Available at: https://www.lastpass.com/ [Accessed 13 May 2022].

Lynch, V. (2017). *Security Changes in Chrome 58 - What You Need to Know*. [online] www.thesslstore.com. Available at: https://www.thesslstore.com/blog/security-changes-in-chrome-58/ [Accessed 12 May 2022].

Microsoft (2022). *Passwordless Strategy - Windows security*. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/passwordless-strategy [Accessed 19 May 2022].

Mossburg, E., Gelinne, J. and Calzada, H. (2016). *Beneath the surface of a cyberattack A deeper look at business impacts*. [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf [Accessed 13 May 2022].

Ollmann, G. (2007). *The Phishing Guide Understanding & Preventing Phishing Attacks*. [online] *cupdf.com*. Available at: https://cupdf.com/document/the-phishing-guide-understanding-preventing-phishing-attacks-ibm-internet.html?page=1 [Accessed 12 May 2022].

Ponemon Institute and IBM Security (2021). *Cost of a Data Breach Report 2021*. [online] *ibm.com*, p.20. Available at: https://www.ibm.com/uk-en/security/data-breach [Accessed 13 May 2022].

Rosenthal, M. (2022). *Must-Know Phishing Statistics: Updated 2022*. [online] *www.tessian.com*. Available at: https://www.tessian.com/blog/phishing-statistics-2020/ [Accessed 12 May 2022].

yubico (n.d.). *How the YubiKey works*. [online] Yubico. Available at: https://www.yubico.com/why-yubico/how-the-yubikey-works/#:~:text=The%20YubiKey%20supports%20one%2Dtime%20passcodes%20(OTP)&text=The%20YubiKey%20communicates%20via%20the [Accessed 18 May 2022].