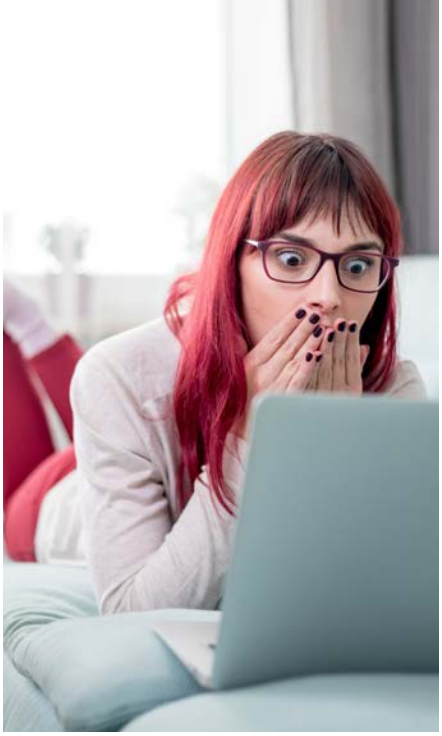
Phishing or Whaling?
Don’t get hooked.
Let’s all be cyber-resilient!



The jargon explained:

"Phishing" is a cyber-attack that uses email or text message as a weapon to obtain your customers' sensitive information. Typically, the fraudster will mimic your website, which is registered under a fake domain name, to obtain your customers' usernames, passwords, bank credentials or credit card details.

"Whaling" is aimed at catching bigger fish than phishing: it's an attack that specifically targets top board members in companies, such as CEOs, CFOs, etc. using the same techniques as phishing.

"Cyber resilience" is a step up from the old cybersecurity. It is now commonly accepted in the business world that it is no longer a matter of "if", but "when" a company will suffer a cyber-attack. Cyber resilience gives a company the ability to prepare for, respond to and recover from cyber-attacks.

But let's take things one step at a time.

How phishing has evolved

Phishing has been around for a few years now. But the fraudsters are getting smarter and faster, while also increasing the frequency of their attacks.

Some key facts about financial fraud and phishing

- Phishing attacks are becoming **more targeted** these days, instead of the global spam campaigns that used to plague our inboxes a few years ago.
- There is a steady growth in **mobile phishing attacks** (+85% year-on-year since 2011).
- The number of phishing sites **using fake HTTPS** security extensions to fool you is increasing rapidly (up by over 50%). HTTPS makes a website look legitimate to the unsuspecting end-user.
- 40% of all phishing is targeted at **financial institutions**, making them by far the largest (and juiciest) target
- 65% of malicious emails target '**credential theft**'. 88% of this theft is carried out using phishing websites.
- **Telephone impersonation** is another phishing technique that is on the rise. With telephone impersonation, fraudsters contact bank call centres or their customers multiple times, each time gaining a different piece of information until they have enough pieces of the ID jigsaw to impersonate an actual bank customer and gain access to their account.

All of this has a huge impact on your business:

$7 billion
+32%

The cost of fraud is estimated to exceed $7 billion for the US alone. This is an increase of 32% over the past 2 years

X 500
in 2 months

Since September 2019, financial fraud resulting from phishing rose by a factor of 500 on a global scale in just 2 months.

Sources: ENISA Threat Landscape Reports,
Phishing Trend and Intelligence reports Phishlabs, ENISA 2020 Cyber Threat Intelligence Bonding EU Event (30-31 Jan 2020)

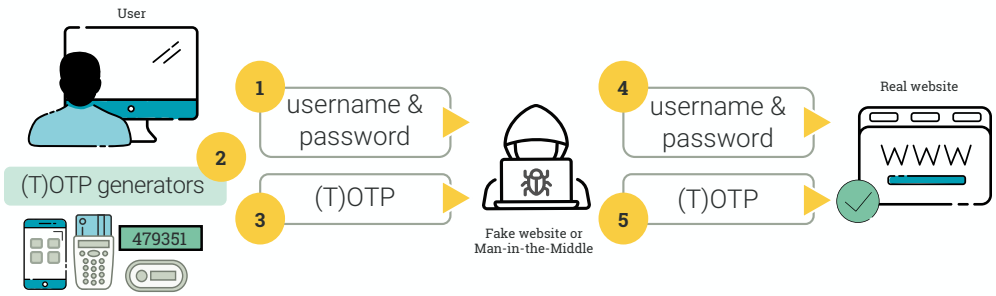
The problem with current authentication methods

Most financial institution and companies use **multiple credentials to authenticate** the customer (bankcard number, customer number, username, password + a One Time Credential, such as a One Time Password generated with the bankcard and card reader).

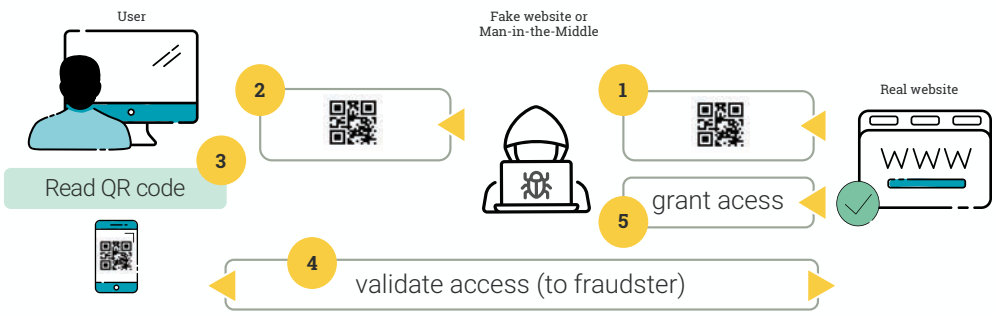
However, **ALL credentials are entered at the frontend** of the financial institution, making them prone to 'Man-In-The-Middle' attacks through phishing websites.

Some of the better-known types of attack are detailed below:

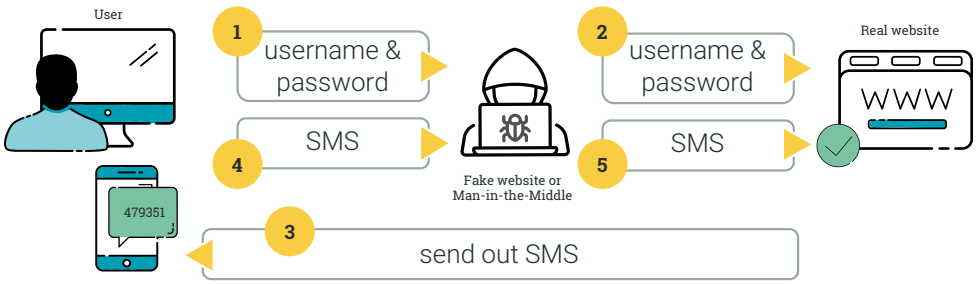
Phishing attack using (Time-based) One-Time Password



Phishing attack using QR code



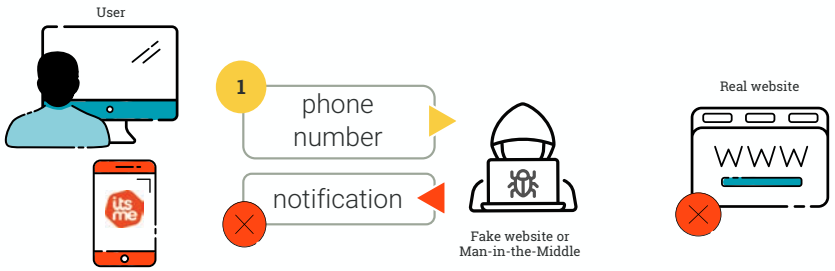
Phishing attack using SMS



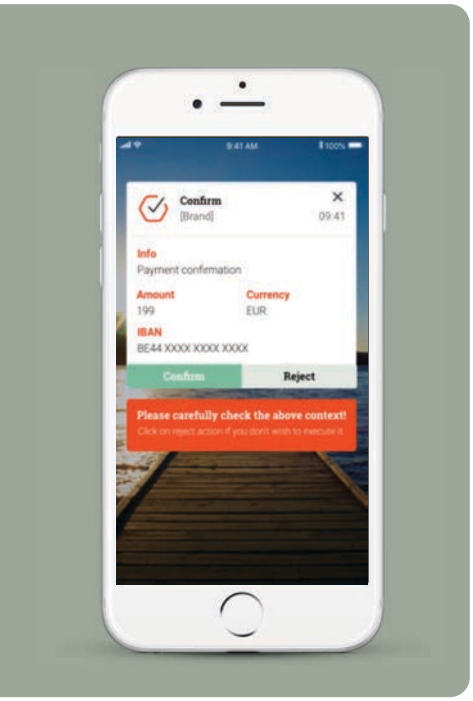
Source: Neowave

Why is itsme® safer than other current means of authentication?

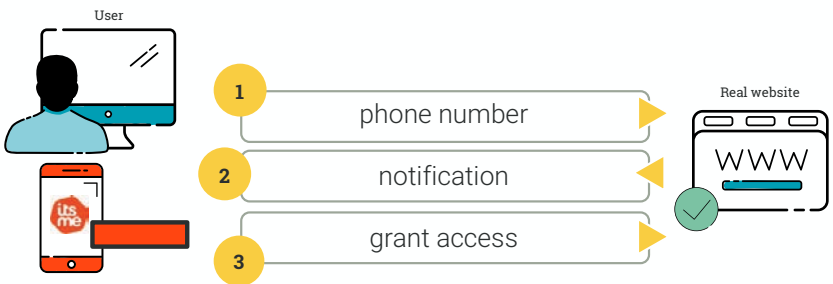
With itsme®, authentication is requested **host to host between the backend of the financial institution and the itsme® backend**. A Man-in-the-Middle phishing website doesn't have a host-to-host connection and so is not able to push a notification in the itsme® app of the user.



With itsme®, authentication is performed **Out Of Band** and sent directly to the user's itsme® app. Because the fraudster has no access to the user's itsme® app or phone, authentication can only be validated by the user himself or herself and the **itsme® credentials are never exposed to the frontend application** of the website.



Each authentication with itsme® is detailed in the app. We apply the "**What You See Is What You Sign**" principle and **dynamic linking** when it's for confirmation of a payment. If a user receives a notification in his/her app that he/she didn't trigger, he/she can refuse it immediately.

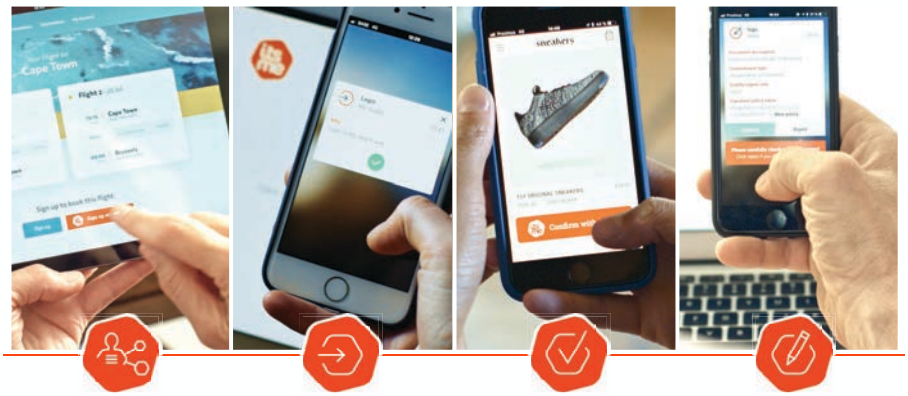


This dramatically increases the complexity of automated Man-in-the-Middle phishing attacks and so makes **using itsme® much more secure**.

What is itsme®?

itsme®, launched in 2017 and used by more than 1,7 million Belgians, is a **digital identity app** that improves the digital experience of your clients.

the itsme® app has become the widely accepted simple and secure standard for mobile identification and the protection of privacy in the digital world.
itsme® enables the following: **identification** (creating a new online account and sharing identity details), **authentication** (secure, personal access to a website or application), **confirmation** of a transaction (approval of an order or bank payment) and, finally, the **legally binding electronic signing** of documents (qualified electronic signature with the highest level of security).



itsme® was granted accreditation by the Belgian government as an official form of digital identity in January 2018 and on a European level in December 2019 (**LOA high eIDAS**). The itsme® app is used extensively in the financial sector among others because it complies with **PSD2, FATF** and **GDPR** guidelines. It has also been awarded **ISO27001** certification.

What is the difference between itsme® and other authentication method next to security?
Other solutions don't give you the opportunity to share a **verified ID data**. itsme® is highly secure, easy to use and respect EU guidelines. It is a standard developed by four Banks and three Mobile Network Operators, with the highest security standards in mind. itsme® is trusted by them and by the Belgian government. So with itsme® you have a secure login AND you know who is really logging into your website or app.

Do you want to know more about the itsme® or do you want to check how you could improve your authentication for your clients? Please contact us and we will be happy to help you out.

Sylvie Vandevelde
Elien Lagast

partner@itsme.be
itsme.be