
BORCELLE

PRESENTATION

PHYSICAL TOKEN 2FA



JANUARY 2050

WWW.REALLYGREATSITE.COM

AGENDA

1 MAIN VULNERABILITIES ↗

2 EASE OF SETUP ↗

3 SPECIAL EQUIPMENT
OR SOFTWARE ↗

4 DEPENDABILITY AND
COMMON PROBLEMS ↗

5 WIDESPREAD
SUPPORT ↗

6 SPECIFIC
SERVICES

MAIN VULNERABILITIES



Phishing attacks: Attackers may trick users into revealing their 2FA codes.
Physical theft or loss: If the token is lost or stolen, someone else could potentially access the user's accounts.
Technical vulnerabilities: Like any technology, hardware tokens can have exploitable flaws

Ease of Setup and Use

Generally, physical tokens are easy to set up. Users typically register the device with their service once, and then use it to generate codes or as a key for authentication. Usability can vary depending on the user’s comfort with technology and the specific token’s design.



Equipment or Software Requirements

Yes, this method requires the user to have a physical token, such as a USB security key or a similar device. Some services may require additional software or apps to register or use the token.



Dependability and Common Problems

Physical tokens are considered highly reliable as they are not as susceptible to remote hacking attempts. Common issues include device malfunction, battery life (for some tokens), and the inconvenience of carrying an additional device².



LOSS OF ACCESS

What Is 2FA (Two-Factor Authentication)?

2FA is an extra layer of protection that requires a second form of ID before logging into an account.



If a user loses their token, they should immediately report the loss to the service provider and follow their procedures, which may include using backup codes or other recovery methods⁴.

WIDESPREAD SUPPORT

Physical token 2FA is supported by many services, especially those that handle sensitive information or require high security.



SETTING UP BROWSERS

1

Setting Up on Google

To set up on Google, go to the 2-Step Verification section in your Google Account settings and follow the prompts to add your physical security key.

2

Setting Up on Yahoo

On Yahoo, access the Account Security page, enable 2-Step Verification, and choose to use a security key

DELIVERABLES

Setting Up on Facebook

For Facebook, navigate to Security and Login Settings, choose Two-factor authentication, and follow the instructions to set up using a security key.

Setting Up on Instagram

Instagram's setup is similar to Facebook's since they are part of the same company. Go to Settings, then Security, and select Two-Factor Authentication to add a physical token.

SETTING UP ON DISCORD

Discord also supports 2FA with physical tokens. Go to User Settings, under My Account, click on Enable Two-Factor Auth, and follow the steps to add your security key. Remember, it's important to keep your physical token secure and to have a backup method in case the token is lost or malfunctions. Always refer to the specific service's documentation for the most accurate and detailed instructions.

DELIVERABLES

PR Rollout

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip. Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Social Media Campaign

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip. Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

TVC

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip. Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

BORCELLE

PRESENTATION

**THANK
YOU.**



JANUARY 2050

WWW.REALLYGREATSITE.COM



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.