TiQR offers NO protection against phishing attacks.

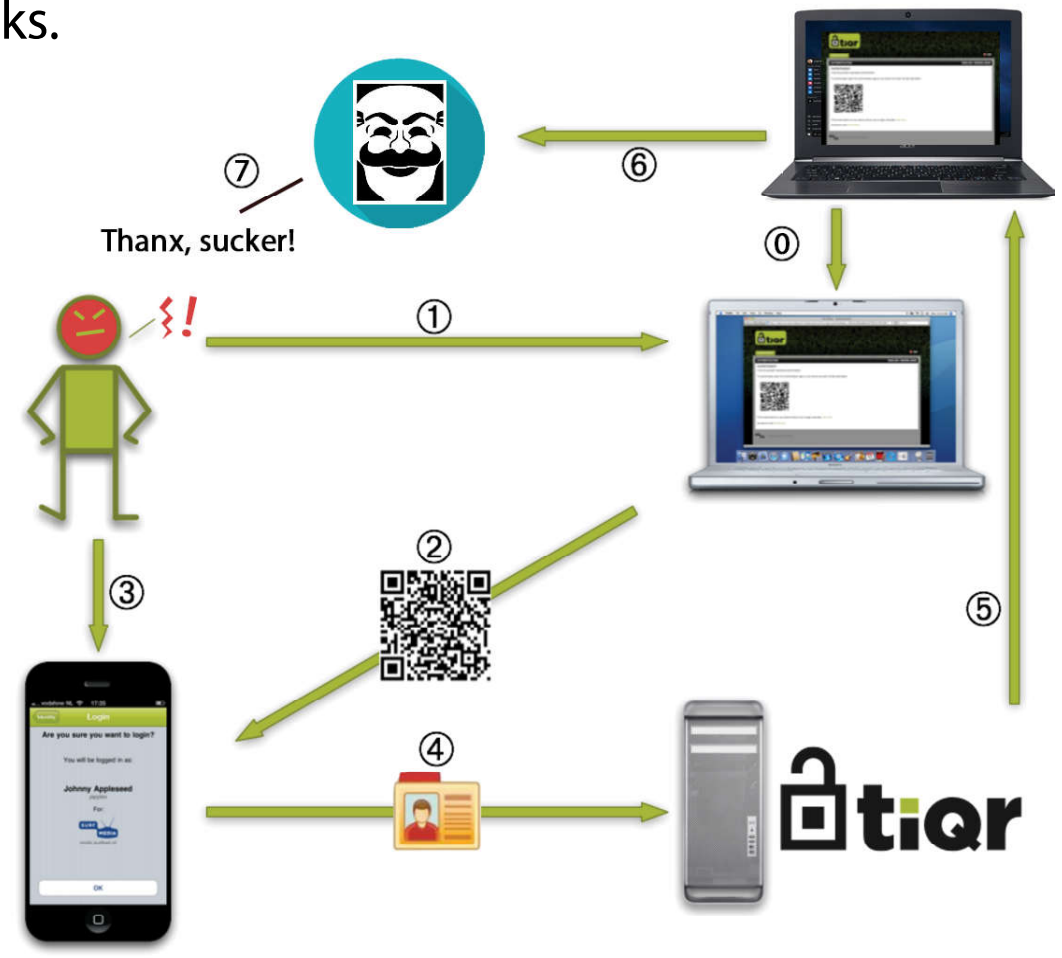
> “TiQR is just like most of QR Code based authentication systems, or like OTP or SMS codes, it only brings the illusion of security. It is just another bullshit.”
>
> Frédéric MARTIN
> https://www.linkedin.com/in/frederic2

The diagram shows the following steps:

1. The user surfs to a web site and is required to log in
2. The web site displays a QR code
3. The user scans the QR code using the tiqr App on his or her phone, confirms login and enters his/her PIN
4. The user's identity together with the response to the challenge encoded in the QR tag is sent to the server using the phone's Internet connection
5. The server validates the response and authorises login
6. The browser reloads the page and the user is logged in

↖ Dream versus Reality ➔

(from official tiqr.org website)



The diagram shows the following steps:

0. Attacker makes a fake website retrieving an official QR code to relay it
1. The user surfs to the fake web site and is required to log in
2. The fake web site displays a QR code
3. The user scans the QR code using the tiqr App on his or her phone, confirms login and enters his/her PIN
4. The user's identity together with the response to the challenge encoded in the QR tag is sent to the server using the phone's Internet connection
5. The server validates the response and authorises login for the attacker
6. The browser reloads the fake page, the attacker is logged in, user is redirected to the official website, as if an error just occured, he has no way to know that his account was just owned by attacker.
7. optional: Attacker can send a nice message to the victim.