Infographic: Unsuccessful Phishing Attack

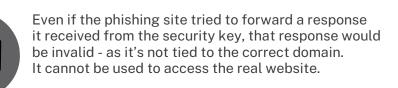
an unsuccessful phishing attack involving a physical security key

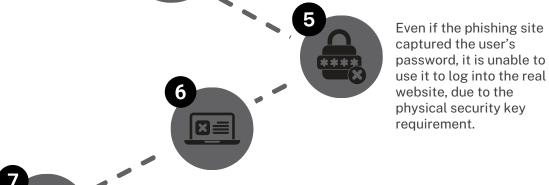


PHISHING ATTEMPT IS UNSUCCESSFUL The phishing site enters the password into

The phishing site enters the password into a real website, which then asks for a response from the user's physical security key. The phishing site cannot supply the response; the attack fails. *The phishing site will give up at this stage - but the following steps are still included to show WHY exactly the attack would fail.

Even if the phishing site asked the user for their physical security key, it would not be able to obtain the correct response from the key, since the phishing site has a different domain than the website where the key was registered.





The adversary behind the phishing website has no access to the user's account - only the user does.

Note that if the legitimate website allows the user to 'authenticate another way' (such as by providing a one-time code from an authenticator app, a backup code, or an SMS code), the phisher could still try to obtain this. This 'downgrading attack' is why programs like **Google's**Advanced Protection Program are useful, as they eliminate phishable authentication methods.



This infosheet was developed in October 2024, for Internews partners and fellows delivering digital security training activities. You are welcome to adapt, edit, or translate this sheet based on your training needs.