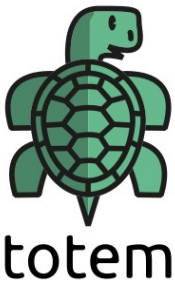
Totem's Phishing Attacks

Phishing Action Card - TP_PM_001



Instructions: If you clicked a phishing link

If you have clicked on a phishing link and entered your login details or credit card information into a fake website:

1. As mentioned already - Do Not Panic.

2. Use a different device (if possible) to log into your compromised account and change your password. If not possible, use the same device.

3. If you entered your credit card information into the phishing page, cancel your card and notify your bank. Where possible, also put a “fraud alert” on your account.

4. If the phishing attack targeted a service provided by Google, Facebook, Twitter or Whatsapp, go to the settings of your account and log out of this account on all connected devices. If you are also using this account (e.g. Gmail or Facebook) to log into other accounts, temporarily remove these accounts’ access as well.

- **Gmail** > go to myaccount.google.com and log in > go to Security > Third Party Apps with Account Access and select “Manage Third-Party Access” > remove access by third parties
- **Facebook** > login > go to Settings > Apps > select the apps you want to remove third party access from > select the app and then select “Remove”
- **Twitter** > login > go to Settings > Apps & Devices > remove access by third party apps and devices
- **Whatsapp** > Open Whatsapp > Go to Settings > select Whatsapp Web > select “Logout from all computers” [https://faq.whatsapp.com/an/web/26000018/]

5. If possible, go to the settings of your account and check that the attacker hasn't entered a strange email address in the auto-forwarding section (email), or changed the phone number or secondary email address the platform uses to verify your account. (If the attacker has entered a different email address or phone number here, they can use this to change your password again, and lock you out of your account).

6. Check that the attacker has not tried to reset the passwords of other accounts linked to your email address (your primary email address is often the way in which services verify it is you, and enable you to reset your password). You can do this by looking closely at the emails you have received since being phished. Are there any "password reset" emails there? Don't forget to check the Trash!

7. If you use the same login details for multiple accounts, change the passwords for each of these accounts as well.

8. Let your contacts and colleagues, or your workplace, know you have been phished, and ask them to be mindful.

9. If the attack was targeted ("spear phishing") - for example, if your organisation has its own email infrastructure and the attack mimicked this - inform the person in the organization who is responsible for IT infrastructure or organizational security.

10. Assess the damage; if possible with the help of a trusted person who will help you think calmly. What information has been compromised? What could someone do with this information? How can you control the damage, or render the information they have useless? (e.g if they got your password, by changing the password and logging out of all devices).

11. If you've been logged out of a Google, Facebook or Twitter account, reach out to the platform. The company might be able to restore your access to your account.

12. If everything else fails, you can reach out to - among others:
    - Access Now Helpline: https://www.accessnow.org/help/
    - Digital Defenders: https://www.digitaldefenders.org/