Целью хакера можете быть вы!

ČESKÁ BANKOVNÍ ASOCIACE

POLICIE ČESKÉ REPUBLIKY

ВНИМАНИЕ! Кто-то запрашивает у вас данные доступа к интернет-банкингу или данные платежной карты от имени вашего банка или полиции Чешской Республики? ИЛИ предлагает совершить платежную операцию из-за неминуемой атаки на ваш счет?

НЕ РЕАГИРУЙТЕ, ЭТО МОШЕННИК! НЕМЕДЛЕННО СВЯЖИТЕСЬ С ВАШИМ БАНКОМ ИЛИ ПОЗВОНИТЕ ПО ТЕЛЕФОНУ 158!

#фишинг #вишинг

5 советов по безопасности ваших денег

1. Никогда и никому не сообщайте данные для входа в систему онлайн-банкинга или номера кредитных карт. Банки не просят их, не рассылают сообщения или электронные письма со ссылками на сайты, где они требуются!

2. Не отвечайте на телефонные звонки, электронные письма или сообщения, в которых кто-то пытается манипулировать вами, заставляя думать, что ваши средства находятся под угрозой и вам необходимо предпринять дополнительные шаги для их сохранения. Если бы ваши деньги были под угрозой, банк давно бы уже отреагировал без вас.

3. Только вы являетесь хозяином своего счета. Не вводите и не подтверждайте в приложении платежи, которые кто-то диктует вам по телефону, не передавайте и не пересылайте никому коды подтверждения из СМС. Аналогично, не давайте никому удаленный доступ к своему компьютеру.

4. Постоянно обновляйте программное обеспечение и антивирус. В том числе и на телефоне!

5. Если вы сомневаетесь, всегда обращайтесь в свой банк или звоните по телефону 158. Имейте в виду, что злоумышленник может подделать любой телефонный номер или электронную почту, (так называемый спуфинг), в том числе номер вашего банка.

#ФИШМНГ - мошеннические сообщения, электронные письма

#безопасныебанки

#ВИШИНГ- звонки фальшивых работников банка