**Эксперт рассказала, как защитить свой счет в онлайн-банке**

***Развитие цифровых финансовых сервисов вынуждает банковских клиентов соблюдать правила цифровой «финансовой гигиены»: своеобразной финансовой техники безопасности, обязательной, в частности, для каждого пользователя онлайн-банка и мобильного банка. Так, стало известно, что в даркнете был выставлен на продажу доступ к коммутатору мобильного оператора - устройства, позволяющего мошенникам перехватывать смс-сообщения от банков и других организаций.***

Но соблюдение довольно простых правил позволит минимизировать риски и защитить банковский счет от посягательств хакеров и кибермошенников. Их назвала для «Российской газеты» эксперт центра финансовой грамотности НИФИ Минфина России Анна Чаплыгина.

***Правила цифровой «финансовой гигиены»:***

1. Установите антивирус на телефон и компьютер.

2. Заходите в личный кабинет на сайте банка или в приложение банка на смартфоне только через защищенный Wi-Fi или мобильный интернет вашего сотового оператора (открытые публичные Wi-Fi-сети не гарантируют конфиденциальности).

3. Скачивайте мобильные приложения только в официальных магазинах (App Store и Google Play).

4. Установите двухфакторную аутентификацию везде, где возможно (и вы будете контролировать списания со счета за счет подтверждений в смс).

5. Используйте защищенные папки на устройствах для персональной информации.

6. Не открывайте вложения в сообщениях от незнакомых адресатов и не предоставляйте в ответных письмах персональную информацию, коды и пароли.

7. Заведите отдельную банковскую карту только для покупок онлайн и не держите на ней значительные суммы (в идеале - переводите ровно столько, сколько требуется для конкретной покупки).

8. Подключите смс-оповещения от банка обо всех операциях по карте (это платная услуга, но со сравнительно небольшой стоимостью; по сути, своеобразная страховка от ситуации, в которой вы можете не узнать о несанкционированном списании вовремя).

9. Используйте приложения для определения входящих вызовов - и не отвечайте подозрительным и незнакомым номерам.

10. Не передавайте платежные данные, пароли и коды из смс-подтверждений третьим лицам; не храните пароли в одном месте явно записанными.

11. Не публикуйте в открытом доступе в соцсетях свои персональные данные (например, номер телефона).

12. Используйте разные пароли для разных сервисов и устройств и регулярно обновляйте их.

*Источник: Российская газета*