НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

КИБЕРБЕЗОПАСНОСТЬ. 9 ПРАВИЛ ПО ЗАЩИТЕ ЛИЧНОГО АККАУНТА ОТ ВЗЛОМА

Чуриев Максат

Старший преподаватель Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Агаева Дурли

Преподаватель Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Чарыева Дунягозел

Преподаватель Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Гайгысызов Довлетгелди

Студент Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

В последнее время информационное поле сотрясают новости о взломах десятков тысяч аккаунтов пользователей по всему миру. У кого-то похищают логин и пароль к банковской учетной записи, кого-то шантажируют похищенной приватной перепиской в социальных сетях.

В основном, во взломе любого аккаунта виноват сам владелец. К этому приводит банальная цифровая неграмотность. Как же избежать взлома учетной записи и защитить конфиденциальную информацию? Для этого необходимо жестко соблюдать основные правила цифровой безопасности.

1. Включите двухфакторную аутентификацию (2FA)

Серьезные интернет-ресурсы позволяют подключить 2FA. При такой авторизации, после ввода учетных данных, требуется ввести код из присланного на телефон сообщения. Без ввода кода зайти в аккаунт не удастся. Для подключения такой аутентификации пользователю требуется привязать телефон или мессенджер к учетной записи.

2. Держите логины и пароли от аккаунтов подальше от посторонних глаз

Очень часто многие совершают следующие грубейшие ошибки:

• Записывают логин и пароль на листок бумаги и приклеивают его на экран монитора, стену или размещают данную информацию в открытом доступе в пространстве около компьютера.

• Записывают логин и пароль в незашифрованный файл и хранят его на компьютере.Делать это категорически нельзя. Информация может стать известной третьим лицам, не только посещающим данное помещение, но и быть попасть к мошенникам при удаленных видеозвонках, фотографировании владельца аккаунта в месте расположения ПК, заражении устройства вредоносным ПО или его взломе.

3. Регулярно меняйте пароль от аккаунта

Пароли от важных учетных записей необходимо менять не реже раза в 6 месяцев. При смене нужно полностью менять комбинацию букв и цифр, а не изменять старый пароль путем добавления или убавления символов.

4. Откажитесь от использования одного и того же пароля на разных сайтах

Это довольно распространенная ошибка, приводящая к «угону» учетной записи. Согласно ежегодным опросам более половины пользователей используют один и тот же пароль для доступа к разным учетным записям. Поэтому, в целях безопасности, избегайте повторного использования одинаковых паролей для входа в несколько учетных записей.

5. Загружайте программы только из официальных источников

Один из старых способов похищения логинов и паролей – это заражение устройства программами-шпионами. После установки на устройство вредоносная программа способна передавать все введенные логины и пароли злоумышленникам. Поэтому не устанавливайте на устройство программное обеспечение с сомнительных сайтов, так как вместе с программой на него может попасть и вредоносное ПО.

6. Регулярно проверяйте устройство на наличие вредоносных программ

Если вы активный пользователь сети, то все устройства необходимо регулярно проверять на наличие вредоносного кода. Почему это необходимо делать часто? Все дело в том, что вредоносное ПО может проникнуть на устройство через загрузку зараженных страниц сайта или через открытие вредоносного вложения к электронному письму. При этом симптомы заражения могут долгое время никак не проявляться.

7. Не входите в учетную запись через общедоступную сеть Wi-Fi

В публичных Wi-Fi-сетях трафик может легко перехватываться. Поэтому откажитесь от авторизации, если выход в Интернет осуществляется через общественную сеть. Если это единственный способ выхода в сеть, то для входа в аккаунт необходимо использовать VPN.

8. Оперативно меняйте пароли при обнаружении вредоносной программы на устройстве

Если на устройстве было обнаружено вредоносное ПО, то пароли от важных веб-ресурсов необходимо изменить как можно скорее. Все дело в том, что с зараженного устройства возможна утечка важной конфиденциальной информации. Именно за ней охотятся кибермошенники, разрабатывающие вредоносные программы.

9. Для входа на сайт используйте только протокол HTTPS

Протокол HTTPS, в отличие от устаревшего HTTP, надежно шифрует передаваемую по сети информацию. Но в Интернете еще много сайтов, не поддерживающих данный протокол. Если вы хотите надежно защитить аккаунт, то используйте при соединениях только HTTPS.