Тема: Безопасность банковских карт и средств на банковских счетах

Практическое задание для самостоятельной работы

Формирование навыков противодействия финансовому мошенничеству

20 Простых правил цифровой финансовой гигиены.

1. Не устанавливайте онлайн-приложения для доступа к банковскому счету на компьютеры, гаджеты, которые используются **для игр, для свободного «серфинга»** по интернету;
2. **Своевременно обновляйте** версии онлайн-приложений для дистанционного банковского обслуживания, антивирусные программы и браузеры. Новые версии, как правило, создаются уже с учетом последних выявленных угроз.
3. Регулярно, не реже раза в полгода **меняйте пароли** для входа в банковское приложение, программы и смартфон.
4. Если вы вошли в интернет- или мобильный банк, **не загружайте параллельно** другие программы.
5. При использовании VPN и подключении к незащищенным сетям Wi-Fi **закрывайте онлайн-приложения банков.**
6. Если вы через компьютер использовали удаленное соединение, то после сеанса работы выйдите из программы удаленного доступа, **обязательно выньте флэшку** с ключом удаленного доступа.
7. **Не открывайте письма, файлы, ссылки,** пришедшие к вам от неизвестных людей, а также «странные» и неожиданные письма от знакомых людей.
8. Если вы заметили **изменение оформления или интерфейса** загрузочной страницы банка или интернет-банка, проверьте правильность написания адреса страницы.
9. Не скачивайте или удалите программы, приложения, которые при установке или обновлении **«требуют» ручного снижения уровня безопасности** вашего устройства.
10. Не пользуйтесь программами интернет-банкинга на компьютерах, установленных **в публичных местах.**
11. Установите обязательно **двухфактурную систему индентификации** на портале Госуслуги и других государственных порталах.
12. **Проверяйте подлинность адресов** интернет-сайтов: неработающие страницы сайта, ошибки на страницах – косвенные признаки мошеннического сайта.
13. Мошенники могут воспользоваться **потерянным или украденным средством мобильной связи.** При наличии на вашем устройстве

возможности поиска пропавшего устройства или возможности дистанционной блокировки и удаления информации заранее уточните информацию у производителя мобильного устройства и мобильного оператора связи.

14. **Сохраните важную для вас информацию с мобильного устройства:** контакты, фотографии, заметки и прочее – на резервном диске для полноценного восстановления вашего мобильного устройства в максимально короткие сроки в случае утраты или хищения мошенниками.
15. Используйте для регистрации в интернете, интернет-магазинах и для иных бонусных и пристальных программ лояльности клиентов **отдельный почтовый ящик.**
16. **При потере телефона,** к которому был подключен мобильный банк, **или смене номера** обязательно оповестите ваш банк об этом факте. В противном случае лицо, которому достанется ваш номер или телефон, будет получать от банка информацию о состоянии вашего счета, а также одноразовые пароли для входа в интернет-банк. Мошенник, обладая мобильным телефоном, который банк использует в качестве контактного, может в течение двух минут заменить неизвестный ему ваш пароль на новый и опустошить ваш счет.
17. В большинстве банков для доступа в мобильный или интернет-банк или подтверждения транзакции требуются **ввести одноразовый пароль,** который присылается на привязанный к этому счету мобильный телефон. Дополнительная мера защиты потребует от вас больше времени для осуществления платежных операций, но существенно обезопасит ваши средства.
18. **Двухключевой доступ к банковским транзакциям:** эта технология позволяет защитить ваш счет от мошенников. Однако, если ваше мобильное устройство, ваша sim-карта или ее дубликат, то счет оказывается фактически беззащитным. Обязательно установите пароль доступа в ваш смартфон. Конечно, он должен отличаться от пароля к онлайн-приложению банка.
19. При выборе паролей доступа следует отдавать предпочтение **паролям из не менее 7 знаков** с использованием различных регистров, в том числе букв и цифр, а также других знаков.
20. В современной жизни количество паролей в приложениях, сайтах, интернет-магазинах, электронной почте, аккаунтах соцсетей и государственным порталам может достигать нескольких десятков. При условии, что все пароли разные, запомнить их будет сложно. Категорически не стоит записывать их в мобильное устройство. Для экстренного доступа к информационным системам записывайте пароли и логины в комфортном месте, **недосягаемом для мошенников.**