ПАМЯТКА ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ КЛИЕНТОВ

Кибербезопасность – обеспечение защищенности киберпространства, в котором функционирует бизнес, которое достигается применением набора средств, методик и принципов, направленных на противодействие угрозам в киберпространстве и минимизацию последствий от их реализации.

Выполнение простых правил кибербезопасности позволит создать общее безопасное киберпространство для достижения совместных целей и сделать сеть Интернет более безопасным местом.

Базовые правила кибербезопасности

1. Будьте осторожны с тем, какую информацию публикуете о себе и о других.

Перед публикацией любой информации в сети Интернет ответьте на несколько вопросов:

- разглашает ли публикация Ваше текущее местоположение или, наоборот, говорит о Вашем отсутствии где-то на протяжении долгого времени?
- нарушает ли публикуемая информация соглашение о конфиденциальности, трудовой договор или иное соглашение, которое Вы подписали?
- содержит ли публикация чужую личную информацию или бездоказательные публичные обвинения?

Если хотя бы на один из вопросов Вы ответили «Да», следует отказаться от публикации данной информации.

2. Используйте несколько факторов аутентификации

Аутентификация – это процесс подтверждения идентификационных данных (например, логина и пароля) путем сравнения предоставленных учетных данных с существующими сведениями об авторизованных пользователях перед получением доступа к системе или приложению. По возможности старайтесь использовать не только пароль, но и дополнительный фактор для аутентификации. Это может быть одноразовый код из СМС-сообщения, электронный сертификат или биометрический фактор (например, отпечаток пальца или распознавание лиц).

3. Используйте надежные и уникальные пароли

Современные вычислительные мощности позволяют вычислить пароль из девяти букв в нижнем регистре за 10 секунд. Хороший пароль, обеспечивающий достаточную надежность, должен состоять не менее чем из 8 символов и содержать цифры, прописные и строчные буквы и символы. При этом лучше всего не использовать целые слова на любом языке, в том числе русские в английской раскладке клавиатуры. Использование уникальных паролей позволит сохранить безопасность остальных сервисов в случае, если пароль от одного из них будет скомпрометирован.

4. Обращайтесь с паролями правильно

Никому не сообщайте свои пароли – даже своим близким и сотрудникам банка.

Не записывайте пароли или PIN-коды банковских карт, либо не указывайте в записи информацию о том, от чего данный пароль, и не храните вместе с картой, а также в месте, которое не находится под Вашим постоянным контролем.

Регулярно меняйте пароли. Рекомендуемая периодичность смены – не реже одного раза в 3 месяца, максимальная – раз в год.

5. Установите антивирусное программное обеспечение и регулярно обновляйте базы сигнатур

Ежедневно появляются сотни новых компьютерных вирусов и вредоносных программ. Избежать заражения позволит установка антивирусного программного обеспечения. Современные антивирусы позволяют распознать новый вирус по его поведению в системе, однако наиболее эффективным является регулярное обновление баз сигнатур – цифровых «отпечатков» вредоносного программного обеспечения.

6. Делайте резервные копии важных данных

Регулярное создание резервных копий гарантирует, что в случае потери данных их можно будет восстановить. При этом следует хранить резервные копии в нескольких местах и на нескольких носителях, чтобы в случае повреждения одной резервной копии была возможность использовать другую.

7. Используйте только безопасное интернет-соединение

Не используйте незащищенные или недоверенные Wi-Fi-сети для совершения онлайн-платежей или передачи важных данных, а также используйте средства защиты соединений (VPN).

Правила кибербезопасности при использовании электронной почты

8. Не отвечайте на подозрительные письма

При получении электронного сообщения о выигрыше в лотерею или о знакомых, потерявших свой паспорт в другой стране, никогда не отвечайте. Письмо предназначено для того, чтобы попытаться украсть информацию о Вас или о Вашем банковском счете.

9. Остерегайтесь фишинга

Фишинг – это вид киберпреступности, когда мошенники связываются по электронной почте с пользователями от имени известных ресурсов (например, OZON, Wildberries, Госуслуги и другие). Под предлогом проблем с учетными записями они просят предоставить конфиденциальные сведения, такие как данные кредитной карты, пароли.

Никогда не переходите по ссылкам в письмах, где Вас просят ввести пароль или другую Вашу личную информацию, только если Вы самостоятельно не запросили смену пароля. Внимательно посмотрите на источник письма и убедитесь, что он является законным, прежде чем что-либо делать.

10. Не открывайте незапрашиваемые вложения

Не открывайте вложения из писем, если отправитель Вам неизвестен, а также если Вы не ожидаете письмо с таким вложением. Открытие файлов из неизвестного источника может сделать устройство уязвимым для злоумышленника.

Если источник письма Вам знаком, но письмо выглядит подозрительно, убедитесь у отправителя по другому каналу связи, например, по телефону.

Правила кибербезопасности при использовании веб-сайтов

11. Не переходите по подозрительным ссылкам

Не открывайте подозрительные ссылки, а также не переходите по коротким ссылкам типа bit.ly, u.to, bit.do и др. Такие ссылки часто используют и присылают мошенники.

12. Обратите внимание на адрес сайта перед вводом своих данных

Фальшивый сайт может полностью копировать внешний вид настоящего, но адрес сайта в строке браузера будет отличаться. Внимательно изучите адрес сайта, поскольку мошенники могут пытаться подделать его путем использования визуально похожих букв или похожего домена.

13. Проверьте наличие на сайте протокола HTTPS

Проверьте наличие знака HTTPS в адресной строке браузера (значок закрытого «замочка» или адресная строка, окрашенная в зеленый цвет) перед передачей любой информации на сайт. Если знак HTTPS отсутствует, туда нельзя передавать никакую информацию.

14. Проверьте подозрительные сайты

Проверить сайт и узнать истинных владельцев сайта возможно через специальные сервисы WHOIS (whois.ru, reg.ru и др.).

15. Когда нельзя вводить данные карты

Никогда не вводите данные банковской карты, код CVV2/CVC2 с задней стороны и коды из СМС от банка при заполнении заявок на социальные выплаты, для получения выигрыша в лотерее и проч. Для оформления выплат или перечисления выигрыша используется номер банковского счета, а не данные банковской карты. Любая просьба ввода данных карты и секретного кода – явный признак мошенничества.

Звонок из банка

16. Я Вам перезвоню

Если Вам звонят и представляются сотрудниками банка, прежде чем предпринимать какие-либо действия, перезвоните сами по номеру, указанному на банковской карте, и уточните, действительно ли Вам звонил сотрудник банка.

17. Онлайн-консультант

Если на сайте или в приложении банка есть возможность обращения к онлайн-консультанту, уточните у него в процессе разговора, действительно ли Вам звонит сотрудник банка.

18. Пароль «Рыба-меч»

Не сообщайте кодовое слово, если не уверены, что разговариваете с сотрудником банка. Зная Ваши персональные данные и кодовое слово, мошенники получат возможность совершать операции с Вашим банковским счетом.

19. Обращайтесь в отделение банка

Не проводите действия по разблокировке Вашей карты, защите Ваших счетов от действий мошенников по указанию звонящих Вам «сотрудников банка», обращайтесь в отделение банка. Запомните, в случае обнаружения подозрительных операций настоящие сотрудники банка не будут звонить Вам, а сразу заморозят операцию или заблокируют карту.

20. Включите в приложении банка проверку телефонных номеров

Мобильные приложения банков предлагают сервисы для проверки телефонных номеров. Включите использование данного сервиса в приложении своего банка.

21. Устанавливайте мобильные приложения банка только из доверенного источника.

Мобильное приложение из магазина приложений Вашего устройства может быть мошенническим. Установить мобильное приложение банка можно только из доверенного источника, например, сайта банка, в отделении банка. А обновить версию приложения можно по ссылке в уведомлении в действующем приложении Вашего банка.

Безопасность на сайтах бесплатных объявлений

22. Проверяйте отзывы

Обратите внимание на профиль продавца. Профили мошенников обычно созданы в течение последних 10 дней (чаще 1-2) и не имеют завершенных сделок в истории.

23. Не переходите для общения в мессенджеры

Ведите переписку только на самом сайте или в приложении. Основная цель мошенников – вывести диалог из-под контроля администрации площадки.

24. Не переходите по присылаемым ссылкам

Старайтесь не переходить по ссылкам, присланным пользователями торговых площадок. По возможности старайтесь использовать предлагаемые площадкой способы доставки, в ином случае переходите на сайт не через направленную ссылку, а попробуйте найти данный сервис через поиск.

25. Безопасная оплата

По возможности используйте функцию «Безопасная сделка» внутри ресурсов с бесплатными объявлениями для оплаты товаров. В иных случаях лучше использовать отдельный телефонный номер, к которому не привязаны мессенджеры, и отдельную виртуальную карту, на которую переводить средства непосредственно перед сделкой в размере суммы сделки. Это лишает злоумышленника возможности прислать фишинговую ссылку и снимать с баланса карты Ваши деньги.