ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1. ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

Для безопасной работы в сети Интернет необходимо соблюдать следующие правила:

1.1. Используйте надежное Интернет-соединение:

Не рекомендуется использовать публичные сети Wi-Fi, особенно для проведения важных действий. Выходя в интернет через общественную сеть Wi-Fi, вы не контролируете ее безопасность, а значит, легко можете стать целью для преступника. При использовании публичных сетей Wi-Fi рекомендуется избегать выполнения финансовых операций и операций с использованием персональных данных – в частности, пользоваться услугами интернет-банка и совершать покупки онлайн.

1.2. Используйте надежные пароли:

Пароли – одно из самых слабых мест в системе информационной безопасности. Пользователи часто создают пароли, которые легко запомнить. Следовательно, злоумышленникам не составляет труда подобрать их с помощью специальных программ. Используя один и тот же пароль для нескольких учетных записей, вы подвергаете свои данные еще большему риску, ведь, получив учетные данные от одного сайта, злоумышленники смогут войти и в другие ваши аккаунты.

1.3. По возможности включите многофакторную аутентификацию:

Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используются два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля при многофакторной аутентификации запрашивается дополнительная информация, например, дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или адрес электронной почты.

1.4. Обновляйте программное обеспечение и операционную систему:

Разработчики постоянно работают над безопасностью продуктов, отслеживая последние угрозы и выпуская исправления безопасности в случае обнаружения уязвимостей в приложениях. Используйте последние версии операционных систем и приложений, чтобы не пропускать свежие обновления безопасности. Это особенно важно для приложений, содержащих платежные данные, сведения о состоянии здоровья и прочую конфиденциальную информацию пользователя.

1.5. Убедитесь в надежности сайта:

Надежность – важный атрибут всех посещаемых веб-сайтов, особенно тех, на которых осуществляются транзакции. В частности, сайтов электронной коммерции. При переходе на неизвестный сайт проверьте, защищен ли он SSL-сертификатом. Адреса таких сайтов начинаются с HTTPS вместо HTTP (буква S означает «безопасный»), а в адресной строке отображается значок замка.

1.6. Следите, по каким ссылкам вы переходите:

Один неосторожный переход по ссылке – и ваши личные данные попали к злоумышленникам или устройство было заражено вредоносной программой. Поэтому важно следить за тем, по каким ссылкам вы переходите, и избегать определенных типов контента: ссылок из ненадежных источников, спам-сообщений, онлайн-викторин, кликбейтных заголовков, «бесплатных» предложений и нежелательной рекламы.

1.7. Убедитесь, что ваши мобильные устройства защищены:

Около 60% пользователей используют мобильные устройства для совершения покупок и поиска информации в интернете гораздо чаще, чем компьютеры, и такие устройства должны быть надежно защищены. Рекомендуется использовать пароли, секретные коды и другие средства безопасности, такие как считывание отпечатков пальцев или технологию распознавания лица на всех устройствах: телефонах, компьютерах, планшетах, умных часах, умных телевизорах и других устройствах.

1.8. Регулярно выполняйте резервное копирование:

Следует иметь резервные копии важной личной информации на внешних жестких дисках и регулярно создавать новые резервные копии. Программы-вымогатели – это тип вредоносных программ, блокирующих компьютер и не позволяющих получить доступ к важным файлам. Резервное копирование данных помогает минимизировать негативные последствия атак программ-вымогателей, а специальное ПО для защиты повысит уровень вашей безопасности.

1.9. Удалите неиспользуемые учетные записи:

У многих есть учетные записи, которые давно не используются. Их наличие может стать источником уязвимостей при использовании интернета. Старые учетные записи часто имеют более слабые пароли, а сайты, на которых они использовались, могут иметь ненадежную политику защиты данных. Кроме того, по данным в старых профилях социальных сетей преступники могут собрать о вас различные данные, например, дату рождения и местонахождение, и использовать их для последующей атаки.

1.10. Будьте осторожны с загрузками:

Цель злоумышленников – заставить вас скачать вредоносную программу, которая откроет им доступ к вашему устройству. Вредоносные программы могут быть замаскированы под любое ПО, начиная с популярных

игр и заканчивая приложениями для проверки погоды или наличия пробок на дороге. Кроме того, они могут быть скрыты на созданных злоумышленниками веб-сайтах, которые пытаются установить вредоносные программы на ваше устройство.

1.11. Будьте осторожны с публикациями:

В интернете нет возможности удаления опубликованной информации. Все опубликованные комментарии и изображения могут навсегда остаться в Сети, поскольку при удалении оригинала вы не удаляете копии, которые могли сделать другие пользователи. После публикации комментария уже нет возможности «взять свои слова обратно», также невозможно удалить опубликованное компрометирующее изображение.

1.12. Будьте осторожны с онлайн-знакомствами:

Ваши интернет-знакомые не всегда являются теми, за кого себя выдают. Они могут даже не являться реальными людьми. Используя поддельные профили в социальных сетях, злоумышленники охотятся за неосторожными пользователями с целью кражи их средств. К социальной жизни в интернете стоит относиться с такой же осторожностью, как и к социальной жизни в реальном мире. Это особенно важно в связи с возросшим в последние годы количеством случаев мошенничества в сфере онлайн-знакомств.

1.13. Перепроверяйте информацию, найденную в интернете:

К сожалению, в интернете присутствует большое количество поддельных новостей и ложных сведений. В потоке получаемой ежедневно информации легко потеряться. Если вы сомневаетесь в достоверности прочитанной информации, проведите собственное исследование и установите реальные факты.

1.14. Используйте хороший антивирус и регулярно обновляйте его:

Важно использовать надежное антивирусное решение. Программное обеспечение для безопасности в интернете защищает устройства и данные и блокирует не только распространенные угрозы, такие как вирусы и вредоносные программы, но и комплексные атаки с использованием приложений-шпионов. Как и в случае с операционными системами и приложениями, антивирус необходимо регулярно обновлять, чтобы получать защиту от новейших угроз.

2. БЕЗОПАСНОСТЬ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

В связи продолжающейся фиксацией фактов рассылок фишинговых писем, проводимых злоумышленниками с целью получения конфиденциальных данных пользователей, внедрения вредоносного программного обеспечения, а также рассылки заведомо ложных сообщений об актах терроризма. Пользователям при работе с электронной почтой сети Интернет необходимо соблюдать следующие правила:

2.1. Внимательно проверяйте электронные письма:

Получив любое письмо, не спешите отвечать или выполнять инструкции из него: сначала обратите внимание на важные детали. Должно насторожить:

- Броская тема. Крупные переводы, денежные компенсации, взлом или блокировка учетной записи, мошеннические операции, банковская деятельность, геополитическая обстановка… Злоумышленники стараются завладеть вниманием, играя на чувствах жертвы, особенно часто — на жадности или страхе.

- Нагнетание обстановки. Фразы вроде «срочно!» и «у вас осталось всего 3 часа», обилие восклицательных знаков — все это уловки злоумышленников, цель которых заставить вас торопиться, паниковать и от этого потерять бдительность.

- С особой осторожностью относиться к письмам, в которых содержаться угрозы или требования к совершению определенных действий («Открой», «Прочитай», «Подтвердить регистрацию» и т.д.).

- Ошибки, опечатки и странные символы в тексте, а также замена части букв на похожие латинские. Это способ обойти спам-фильтры.

- Странный адрес отправителя. Нагромождение случайных букв и цифр. Или неверно указанный домен в адресе отправителя письма с именами известных почтовых сервисов с небольшим изменением, например: mayl.ru или qoogle.com — признаки фишинговых писем.

- Ссылка в письме, если она там есть. Точнее, адрес сайта, на который она ведет. Чтобы увидеть его, нужно навести мышку на ссылку и внимательно проверить адрес.

- Вложения. Фишинговые письма могут содержать вложения в виде файлов с вредоносным программным обеспечением.

- Просьбы о предоставлении личной информации. Фишинговые письма могут содержать требования о предоставлении логинов, паролей, номеров банковских карт другой конфиденциальной информации.

2.2. Что делать, если Вы обнаружили фишинговое письмо?

- Внимательно проверить адрес отправителя письма.
- Не нажимайте на ссылки, если они заменены на слова.
- Не скачивайте вложения из писем, если вы не уверены в их подлинности.
- Не открывайте и не скачивайте вложения, особенно, если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями EXE, COM, PDF, RTF, LNK, CHM, VHD.
- Не загружайте картинки, содержащиеся в письмах, полученных из незнакомых вам источников.
- Внимательно относиться к письмам на иностранном языке.
- Не пересылайте письма коллегам, родственникам и иным лицам.
- Удалите фишинговое письмо.

2.3. При поступлении на адрес электронной почты заведомо ложного сообщения об акте терроризма необходимо принять следующие меры:

- Поступившее сообщение об акте терроризма не удалять.
- Осуществить копирование текста сообщения об акте терроризма в виде снимков экрана устройства (скриншотов либо фотоизображений, полученных посредством цифровой фото фиксации).
- На скриншотах (фотоизображениях) должна отображаться следующая информация об объекте:

- название темы письма;
- адрес электронной почты отправителя письма;
- дата и время отправления письма;
- полный текст письма;
- вложения в виде файлов;

- При невозможности фиксации сообщений об акте терроризма в виде скриншотов/фотоизображений осуществить их фиксацию посредством функций копирования и вставки в документ Word (с сохранением указанной

информации об объекте).

- О поступившем сообщении об акте терроризма незамедлительно сообщить старшему дежурному оперативному БГУ по телефону (3952) 500008, доб. 151, ожидать дальнейших инструкций.

3. ЗАЩИТА ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

Чтобы не стать жертвой телефонных мошенников, никогда не сообщайте по телефону свои личные данные (паспорт, CVV-коды, коды из SMS), не переходите по подозрительным ссылкам, не устанавливайте приложения из неизвестных источников и не переводите деньги незнакомцам. Если звонок кажется подозрительным, немедленно прервите разговор, положите трубку и сами перезвоните в организацию, от имени которой звонили, чтобы проверить информацию.

Золотое правило: "Бесплатный сыр только в мышеловке". Действуйте обдуманно и не торопитесь, а главное – никому не сообщайте свои конфиденциальные данные и коды.

3.1 Чего категорически нельзя делать:

- Сообщать конфиденциальные данные:
  Никогда не сообщайте пин-коды, CVV/CVC-коды, коды из СМС, пароли, номера банковских карт и другую личную информацию.

- Переходить по ссылкам и устанавливать приложения:
  Не открывайте SMS с неизвестными ссылками и не устанавливайте приложения из непроверенных источников.

- Переводить деньги на "безопасные счета":
  Не доверяйте предложениям о "специальных безопасных счетах", куда якобы нужно перевести деньги для их сохранности. Никаких "специальных безопасных счетов" в банках – НЕ СУЩЕСТВУЕТ!

- Верить угрозам и срочности:
  Банки и правоохранительные органы никогда не требуют срочно перевести деньги или совершать действия по телефону под угрозой уголовной ответственности.

- Перезванивать на незнакомые номера:
  Если вы получили подозрительное SMS, не перезванивайте на номер, с которого оно пришло.

3.2 Действия при подозрительном звонке:

- Прервать разговор:
  Если вы получили подозрительный звонок, положите трубку и не продолжайте разговор.

- Самостоятельно перепроверять информацию:
  Если звонок поступил от имени банка или родственника, самостоятельно перезвоните им по официальному номеру, чтобы убедиться в правдивости информации.

- Связаться с близкими:
  Обсудите ситуацию с друзьями или родственниками.

- Обратиться в банк самостоятельно:
  Если вам звонят из банка и просят совершить какие-либо действия, сами позвоните на горячую линию банка, а не следуйте инструкциям звонящего.

- Потребовать вызвать повесткой:
  Если звонящий вам представился сотрудником правоохранительного органа (Полиция, ФСБ и т.д.) и требует от вас совершить определенные действия или сообщить интересующую его информацию в рамках проводимой проверки. Вежливо попросите вызвать вас для опроса официальной повесткой в отдел, где вы дадите все необходимые объяснения.

3.3. Распространенные сценарии мошенников:

- Звонок "из банка" или "полиции":
  Убеждая, что на вас оформлена кредитная заявка или на вас совершаются подозрительные операции, мошенники пытаются заставить вас взять кредит и перевести деньги на их "безопасный счет".

- Допуск к сессии и экзаменам:
  Учащемуся ВУЗа поступает звонок якобы из деканата, учебного отдела и т.д. Говорят, что нужно зарегистрироваться на образовательном портале, для допуска к экзаменам, подтверждения документа об образовании и т.п. После этого требуется продиктовать одноразовый код. На самом деле это код от «Госуслуг». Так взламывают личный кабинет, чтобы взять на имя студента кредиты или использовать информацию о нем в других преступных схемах.

- Предложения от лжеброкеров:

Обещание легких денег многих привлекает. Злоумышленники связываются с потенциальными инвесторами через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое – нужно лишь открыть «брокерский» счет и инвестировать деньги. Доход – не меньше миллиона.

- Поручение руководителя:
  Злоумышленники оформляют поддельный профиль в мессенджере, используя взятые из открытых источников настоящие ФИО и фото директора компании или непосредственного руководителя сотрудника. Сотруднику поступает сообщение в мессенджер или звонок на телефон якобы от имени руководителя. Тот предупреждает о предстоящей проверке со стороны ответственных организаций: ФСБ, Росфинмониторинга, МВД и др.

- Заканчивается срок действия договора с сотовым оператором:
  Мошенники связываются с вами по телефону от имени сотового оператора и сообщают об окончании срока действия договора на услуги связи. Для его пролонгации вам отправляют код в СМС, который запрашивают мошенники и который на самом деле нужен для входа в ваш личный кабинет Госуслуг.

- Подтвердите стаж для получения пенсионных выплат:
  Злоумышленники звонят пожилым людям и представляются сотрудниками Социального фонда России (СФР). Сообщают, что обнаружен неучтённый трудовой стаж, который мог бы увеличить размер пенсии. Чтобы решить вопрос, надо записаться в отделение СФР или в центр «Мои документы», это сделает «сотрудник», если вы назовете паспортные данные, СНИЛС, ИНН и код из СМС. На самом деле эта информация нужна мошенникам для получения доступа к Госуслугам.

- Связь со знакомым:
  Звонок "из-за срочной проблемы" у родственника, который якобы попал в беду и просит деньги на взятку или решение проблемы.