Приложение к приказу
№ 310-А от 09.04.2024

ПАМЯТКА
о цифровой гигиене и противодействии мошенничеству для работников ФГБОУ ВО «Марийский государственный университет»

О цифровой гигиене

Цифровая гигиена – это свод правил для обеспечения информационной безопасности в сети Интернет. Рекомендуется:

1. Устанавливать обновления операционных систем и программного обеспечения. Обновления устраняют опасные недостатки программного обеспечения и уязвимости.

2. Использовать антивирус для выявления вредоносных программ, которые могут нанести вред устройству или привести к потере данных.

3. Использовать длинные и надежные пароли, а также биометрию и двухфакторную аутентификацию. Рекомендуется не использовать единый пароль для всех аккаунтов.

4. Не переходить по сомнительным ссылкам даже от знакомых людей.

5. Личные данные размещать только по необходимости, т.к. они являются основой целевых атак.

6. Соблюдать правила этикета при общении в социальных сетях: не оскорблять, не участвовать в коллективной травле, не отвечать на хамство.

7. Не высказываться негативно об университете, коллегах и руководстве, не выкладывать видео и фото коллег без их согласия.

8. Не писать посты от имени университета (если это не является вашей функцией).

9. Не комментировать посты об университете, чтобы комментарии не воспринимались как официальная позиция университета.

О противодействии мошенникам

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Чаще всего в сети телефонных мошенников попадаются пожилые или доверчивые люди. Для того, чтобы не стать жертвой мошенничества, необходимо следовать простым правилам безопасности.

Основные схемы телефонного мошенничества

1. **Обман по телефону: требование выкупа**

КАК ЭТО ОРГАНИЗОВАНО:

Звонок с незнакомого номера от мошенника, который представляется родственником или знакомым и сообщает о задержании сотрудниками полиции и обвинении в совершении преступления (ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений, убийство). Затем в разговор вступает подставной сотрудник полиции с предложением о решении данного вопроса за определенную сумму, которую необходимо привезти в оговоренное место или передать какому-либо человеку.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Обман по телефону с требованием выкупа организуется группой преступников. Телефонный мошенник может находиться как в исправительно-трудовом учреждении, так и на свободе. Телефонные номера набираются наугад, произносится заготовленная фраза, далее мошенник действует по обстоятельствам. В случае согласия жертвы на предоставление указанной суммы, звонящий называет адрес для доставки денег. Часто от мошенников поступают предложения о снятии недостающей суммы в банке. В данном случае мошенники стараются запугать жертву, ведут непрерывный разговор вплоть до получения денежных средств. После получения денег мошенник сообщает о месте нахождения родственника или знакомого жертвы.

ВАШИ ДЕЙСТВИЯ В ДАННОЙ СИТУАЦИИ:

Прервать разговор, перезвонить родственнику, знакомому. В случае отключения телефона необходимо связаться с его коллегами, друзьями и

родственниками для уточнения информации. Следует помнить: если незнакомый человек звонит Вам с требованием привезти на некий адрес денежную сумму – это мошенник. Если звонок поступил от родственника или знакомого с просьбой о помощи (ДТП, возбуждение уголовного дела и т.д.) и просят передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, необходимо уточнить: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба. При разговоре якобы с представителем правоохранительных органов, уточните, из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

МВД РФ обращает ваше внимание на то, что требование взятки является преступлением.

2. SMS-просьба о помощи

SMS-сообщения позволяют упростить схему обмана по телефону. Данный вид мошенничества часто применяется в отношении пожилых людей или слишком юных владельцев телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт.

КАК ЭТО ОРГАНИЗОВАНО:

Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

ВАШИ ДЕЙСТВИЯ В ДАННОЙ СИТУАЦИИ:

Не реагировать на SMS с незнакомых номеров, т.к. это могут быть мошенники, телефонный номер-грабитель. Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества.

КАК ЭТО ОРГАНИЗОВАНО:

От мошенников приходит SMS с просьбой перезвонить на указанный номер мобильного телефона (помощь другу, изменение тарифов связи, проблемы со

связью или с вашей банковской картой и т.д.). В случае, если вы перезваниваете, Вас долго держат на линии. После отключения оказывается, что с Вашего счёта списаны крупные суммы.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

ВАШИ ДЕЙСТВИЯ В ТАКОЙ СИТУАЦИИ:

Не перезванивать по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

3. Простой код от оператора связи

КАК ЭТО ОРГАНИЗОВАНО:

Поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки Вашего оператора мобильной связи. Обоснования этого звонка или SMS могут быть самыми разными:

- предложение подключить новую эксклюзивную услугу;
- для перерегистрации во избежание отключения связи из-за технического сбоя;
- для улучшения качества связи;
- для защиты от СПАМ-рассылки;
- предложение принять участие в акции от вашего сотового оператора.

Мошенник предлагает набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Предложенный мошенником код является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет

злоумышленников. В случае, если Вы наберете данный код, то Ваш счёт будет опустошён, а услуга не будет подключена.

ВАШИ ДЕЙСТВИЯ В ДАННОЙ СИТУАЦИИ:

Необходимо перезвонить своему мобильному оператору для уточнения условий изменения тарифного плана.

В случае получения SMS-сообщения не спешить выполнить просьбу, а необходимо позвонить оператору связи и узнать о сумме списания с вашего счета при отправке SMS или звонке на указанный номер, сообщить о полученном SMS-сообщении для определения оператором отправителя SMS-сообщения и блокировке его аккаунта.

4. Штрафные санкции и угроза отключения номера

КАК ЭТО ОРГАНИЗОВАНО:

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает о нарушении условий договора:

абонент сменил тарифный план, не оповестив оператора;

не внес своевременно оплату;

воспользовался услугами роуминга без предупреждения и так далее.

Чтобы предотвратить отключение номера, Вам предлагается:

перевести на свой номер сумму штрафа и набрать код;

перевести средства на указанный номер.

Это делается якобы для доказательства своей невиновности сохранения номера телефона.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Т.к. данный телефонный номер Вам необходим, мошенник запугивает Вас. В результате он получает возможность присвоить себе Ваши средства напрямую со счёта телефона.

ВАШИ ДЕЙСТВИЯ В ДАННОЙ СИТУАЦИИ:

Рекомендуется перезвонить своему мобильному оператору для уточнения условий, т.к. никто не имеет права требовать выплаты штрафа, пока Ваша вина не будет доказана. Помните, что у Вас есть права, которые защищаются законом.

Ошибочный перевод средств

КАК ЭТО ОРГАНИЗОВАНО:

На телефон поступает SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплаты услуг. Затем поступает звонок с сообщением об ошибочно переведенных на Ваш счет денежных средствах и просьбой вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Если Вы переводите деньги, то такая же сумма списывается с Вашего счёта.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Для списания во второй раз суммы с Вашего счёта злоумышленник использует чек, выданный при переводе денег. Он обращается к оператору с заявлением об ошибочном внесении средств и просьбой перевести их на свой номер. В первый раз Вы переводите деньги по его просьбе, а во второй раз он получает их по правилам возврата средств.

ВАШИ ДЕЙСТВИЯ В ДАННОЙ СИТУАЦИИ:

Необходимо помнить, что для ошибочно переведенной суммы используется чек. Слова о потерянном чеке свидетельствуют о том, что с Вами общается мошенник.

МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Банковская карта – инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Простота использования банковских карт оставляет множество лазеек для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

На телефон поступает сообщение о блокировке Вашей банковской карты. Предлагается бесплатно позвонить на определенный номер для получения подробной информации. В случае Вашего звонка по указанному телефону сообщают о сбое на сервере, отвечающем за обслуживание карты, и просят сообщить номер карты и ПИН-код для ее перерегистрации.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

В случае сообщения мошеннику номера карты и ПИН-кода деньги с Вашего счета будут сняты.

ВАШИ ДЕЙСТВИЯ В ДАННОЙ СИТУАЦИИ:

Никому не сообщайте реквизиты Вашей карты! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для проверки поступившей информации о блокировании карты необходимо позвонить в клиентскую службу поддержки банка.

Управление «К» МВД РФ рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

1. **ПИН-КОД – КЛЮЧ К ВАШИМ ДЕНЬГАМ**

Необходимо помнить:

- ПИН-код это ключ от сейфа с Вашими средствами;

- ПИН-код нельзя хранить рядом с картой и тем более записывать ПИН-код на карте;

- никогда и никому не сообщайте ПИН-код.

2. **ВАША КАРТА – ТОЛЬКО ВАША**

Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.

3. **НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД**

В случае звонка из какой-либо организации или получения письма по электронной почте (в том числе из банка) с просьбой о сообщении реквизитов карты и ПИН-кода под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите

по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

4. НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ ПРИ ЕЕ УТЕРЕ

В случае потери карты срочно свяжитесь с банком, выдавшим карту, и сообщите о случившемся, следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

5. ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ

При проведении операций с картой пользуйтесь только банкоматами, расположенными в безопасных местах и оборудованными системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

6. ОПАСАЙТЕСЬ ПОСТОРОННИХ

При совершении операции с пластиковой картой следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом. При наборе цифр ПИН-кода необходимо прикрывать клавиатуру руками. Реквизиты и любая прочая информация о сумме средств и вводимых в банкомат цифрах могут быть использованы мошенниками.

7. БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»

Необходимо обращать внимание на картоприемник и клавиатуру банкомата. В случае, если они оборудованы какими-либо дополнительными устройствами, то лучше воздержаться от использования данного банкомата и сообщить о своих подозрениях по указанному на нём телефону.

8. БАНКОМАТ ДОЛЖЕН БЫТЬ ПОЛНОСТЬЮ ИСПРАВНЫМ

В случае некорректной работы банкомата (долгое время находится в режиме ожидания, самопроизвольно перезагружается) откажитесь от его использования. Есть вероятность того, что он перепрограммирован злоумышленниками.

9. НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.