Алгоритм действий для образовательных организаций по предупреждению мошенничества

10 фраз, которыми начинают разговоры мошенники:

1. От вас поступила заявка на кредит
2. Вы подали заявку на замену телефона, к которому привязана карта
3. Вы выиграли ценный приз
4. С вашей карты пытались списать деньги
5. Ваш родственник попал в беду и просит перевести деньги
6. Мы переведем деньги на счет, с которого можно снимать валюту без ограничений
7. Мы переоформим ваш вклад под более выгодные проценты
8. Мы звоним вам из Центробанка (ФСБ, прокуратуры, полиции)
9. Мы проводим акцию по обмену на рубли бонусных баллов
10. Мы проводим акцию по выявлению карт, чьи данные утекли в интернет

Будьте бдительны при совершении действий с банковскими картами и соблюдайте элементарные правила безопасности, чтобы не стать жертвой мошеннических действий

ПАМЯТКА №2

Ваши действия в следующих случаях:

1. **Звонок с государственного учреждения**. Вам звонят (или пишут в WatsApp, Telegram) и выясняют конфиденциальную информацию или просят совершить ряд финансовых операций. Ни в коем случае не предоставляйте никакие данные, не сообщайте никакую известную вам личную информацию, не перечисляйте деньги! Важно помнить, что органы власти всегда действуют через официальные каналы и никогда не требуют по телефону от граждан каких-то действий.
2. **Блокировка банковской карты**. Вам поступил звонок (сообщение) о блокировке банковской карты или о подозрительных операциях с деньгами – это МОШЕННИК. Прекратите разговор. Не поддавайтесь на возможную уловку преступника и обязательно перезвоните на горячую линию в банк. Там вы получите достоверную информацию о Вашем финансовом счете.
3. **Звонок о несчастном случае**. Вам позвонили от имени близкого человека (родственника), сообщили о несчастном случае и требуют деньги – это МОШЕННИК. Прекратите разговор, не впадайте в панику. Обязательно перезвоните своим близким или знакомым. Убедитесь, что с ними все в порядке. Если телефон отключен, постарайтесь связаться с его близкими друзьями либо коллегами.

4. **Объявление о продаже**. По вашему объявлению о продаже товара в Интернете Вам позвонил покупатель и попросил сообщить реквизиты банковской карты и смс-код, чтобы перевести деньги – это МОШЕННИК. Прекратите разговор и ни в коем случае не сообщайте номер банковской карты и её код. В социальных сетях, на сайтах «Авито», «дом.ру», доверчивым покупателям предлагают внести предоплату за несуществующий товар, однако потом лжепродавец не выйдет на связь. Вас обманывают.
5. **Сообщение в социальной сети**. Ваш друг (родственник) пишет Вам в социальной сети с просьбой срочно перевести в долг деньги или сообщить данные Вашей карты, чтобы перечислить их Вам, скорее всего – это МОШЕННИК.

ПАМЯТКА №3

Самые распространенные виды телефонного мошенничества:

1. Мошенники рассылают сообщения с мольбой – **ребенку нужен донор**. В SMS указывается номер, куда нужно позвонить в случае согласия. При звонке со счета владельца снимаются дополнительные средства.
2. «Оператор» звонит лично и сообщает **о проблемах с вашим счетом**. На предложенный номер предлагает отправить SMS. Проблемы со счетом появляются как раз после отправленного сообщения.
3. «От оператора» приходит SMS. Предлагается позвонить на некий номер и **получить на свой счет 3 доллара**. Деньги приходят, но при этом сам звонок обходится в 5-10 долларов.
4. На телефон приходит SMS **«Привет, как дела?»**. Разговорчивый абонент может продлить переписку вплоть до отрицательного баланса в пользу тайного собеседника.
5. Абоненту звонит молодой человек и обьясняет, что случайно **положил деньги не на свой, а на его счет**. Настойчиво, но вежливо мошенник будет упрашивать перевести ему такую же сумму в ответ.
6. На телефон приходит послание: «**Отправьте SMS на короткий номер, и Вы перейдете на более выгодный тариф**». Все звонки по Московской области станут для вас безлимитными.
7. На улице подходит **незнакомец и просит позвонить с вашего мобильного**. Злоумышленник звонит с него на платные номера.
8. Абоненту звонят **с неизвестного номера**. Он из любопытства перезванивает, но платит за это соединение гораздо больше, чем за обычный звонок по тарифу.
9. Абоненту приходит SMS: « **Кинь денег, друг! Это очень срочно! Я не могу до тебя дозвониться**!». Подобные сообщения приходят с незнакомых номеров.
10. Абоненту сообщают по телефону, что он **выиграл приз от компании – оператора**, но чтобы его забрать, надо купить карту оплаты. После этого

абонента якобы переводят на автоматическую систему пополнения счета. По тоновым сигналам мошенники вычисляют код карты и переводят деньги на свой счет. Будьте внимательны при получении SMS- сообщения «Вы выиграли!». Со 100% вероятностью оно содержит ссылку на некий Интернет – ресурс, благодаря которому, Ваш гаджет будет заражен вредоносной программой. В результате это даст доступ мошенникам к Вашей банковской карте!

11. **«Вам предоставлена компенсация».** Звонок от неизвестного абонента о полагающейся Вам компенсации за приобретенный ранее товар может оказаться ловушкой. Перепроверьте данное сообщение, перезвоните в магазин, где Вы совершили покупку!

ПАМЯТКА №4

Злоумышленников интересуют:

- *Реквизиты Вашей банковской карты, включая PIN – код, CVV2/CVC2 код;*
- *Ваши паспортные данные;*
- *Аккаунты и пароли к социальным сетям, Email;*
- *Полный доступ к электронному финансовому счету в банке.*

ЗАПОМНИТЕ! В любом случае, общение с неизвестным абонентом требует особого внимания! Будьте бдительны! В случае, если вы пострадали от действий телефонных мошенников немедленно обратитесь в ПОЛИЦИЮ!

Всю информацию о том, как не попасть на уловки мошенников, вы можете узнать на официальном сайте МВД по Республике Башкортостан по адресу: www.02.мвд.рф.