Памятка посвящена таким видам мошенничеств, от которых страдают выпускники школ и студенты. За последнюю неделю эта проблема стала особенной острой. Хотя раньше традиционно считалось, что под прицелом мошенников находятся более возрастные категории граждан.

Денежные средства с телефона матери злоумышленникам перечислила 15-летняя школьница. Накануне в мессенджере ей позвонила неизвестная девушка, которая сообщила, что перед предстоящим ОГЭ проверяет данные учащихся, и, якобы, в фамилии девятиклассницы обнаружена ошибка. Она попросила подростка озвучить код, который поступит ей на телефон, чтобы сверить все данные. После того, как школьница назвала его, последовала целая череда новых звонков. Звонил «специалист» портала «Госуслуги», который рассказал о подозрительных действиях в личном кабинете, далее непонятный финансовый инспектор и даже, якобы, сотрудники ФСБ. Все эти «специалисты» убедили ее перечислить денежные средства. В процессе общения злоумышленники присылали ей различные бланки для заполнения. В итоге введенная в заблуждение таким количеством информации несовершеннолетняя со смартфона мамы перечислила несколькими переводами на неизвестные счета 330 000 рублей. После чего аферисты убедили школьницу удалить всю переписку с ними.

Одна из самых частых схем: выпускникам звонят, якобы, из образовательной организации, просят зарегистрироваться на образовательном портале и назвать код авторизации. Таким образом, злоумышленники опять же получают доступ к Госуслугам. С такими аферистами на днях столкнулась студентка Алтайского педуниверситета. После этого на девушку вышли якобы сотрудники Роскомнадзора, ФСБ, службы финансового мониторинга. Сообщили, что некий гражданин Украины, находящийся в розыске, от её имени перевёл деньги на финансирование ВСУ. А девушка автоматически стала соучастницей. На связи со злоумышленниками студентка была четыре дня. Она оформила кредит, но не перевела деньги. Ее смутил «безопасный» счет. Она зашла в интернет, чтобы разобраться, что это за счет, и поняла, что это мошенники. На ресурсах достаточно информации, где разъясняется, что никакого «безопасного» счета нет. Таким способом действуют преступники.

Шантаж тоже является средством влияния на жертву. В данном случае – на молодого человека. Более 900-т тысяч рублей перечислил мошенникам учащийся Алтайской академии гостеприимства. Ему поступил звонок из, якобы, Минобра. Лжесотрудник сообщил, что ему хотят направить письмо через почту и попросил назвать пришедший код. Далее по классической схеме: позвонил «сотрудник» Роскомнадзора, сообщил, что его страница на Госуслугах взломана. Якобы с использованием этих данных от имени его отца был осуществлен перевод в недружественную страну. И теперь его отец понесет наказание. И молодой человек, поддавшись на угрозы и шантаж, зная, где находятся накопления у родителей, пятью платежами через банкоматы перевел деньги на продиктованные мошенниками счета. При этом он был уверен, что спасает и отца, и деньги семьи.

На сегодняшний день также набирает популярность такая разновидность схемы мошенничества,  когда злоумышленники представляются сотрудниками ВУЗа. В данном случае обман происходит следующим образом: злоумышленники звонят на сотовый телефон потенциального потерпевшего (как правило, студента либо абитуриента), поясняют, что для получения домашних заданий необходимо зарегистрироваться на сайте «Открытое образование». После регистрации потерпевшего на указанном сайте, молодым людям приходят СМС-сообщения с кодами доступа, которые якобы необходимо ввести на данном сайте. И это вновь код для доступа к личному кабинету портала «Госуслуги». Информации поступает так много, что молодой человек не успевает сориентироваться. Далее подключаются злоумышленники, представляясь сотрудниками «Роскомнадзора», которые сообщают, что ваша страница на «Госулугах» взломана и поясняют, что денежные средства потерпевшего находятся под угрозой, вследствие чего их необходимо обезопасить, переведя их на так называемый «безопасный» счет.

Еще один способ обмана, который фиксируется несколько недель в крае – звонки от имени сотрудников отделения «Почты России».  Многие молодые люди делают дистанционные покупки и заказы через разные платформы. Злоумышленники поясняют, что потенциальной жертве пришло письмо и для того, чтобы его получить, необходимо назвать код доступа, который пришел в СМС-сообщении. Потерпевший соглашается, называет код доступа, вследствие чего у потенциальных преступников также появляется возможность входа в чужой личный кабинет портала «Госуслуги».

Эти схемы варьируются. Молодым людям звонят под различными предлогами, якобы, из деканата или какой-то образовательной организации, обучающих онлайн-платформ, различных центров обучения, якобы, с целью проверки, коррекции данных или регистрации в сервисе, просят назвать код авторизации, который на самом деле, как уже было сказано, дает злоумышленникам несанкциониродоступ к Госуслугам. Несколько дней назад 11-класснику из 76 школы, что на Южном в городе Барнауле позвонили, якобы, из Минобразования и отчитали, что он до сих пор не зарегистрирован на портале, а соответственно не пройдет аттестацию. Затем предложили зарегистрироваться и помочь сделать это как можно быстрее. При этом девушка-мошенница попросила его включить демонстрацию экрана. И хотя изначально молодой человек решил сделать это через компьютер, она настояла, что первый шаг нужно делать через телефон. Естественно предложили внести в подложную форму регистрации, которая ему тут же была выслана, все персональные данные, паспорт, СНИЛС и код. Который оказался кодом от Госуслуг. Вскоре молодой человек стал получать многочисленные уведомления из банков и микрофинансовых организаций, так как мошенники мгновенно вошли в личный кабинет и стали рассылать заявки на кредиты. Школьник позвонил отцу, который вместе с ним немедленно лично направился в МФЦ, и все несанкционированные операции были пресечены.

Цель в каждом таком случае одна - получение доступа к аккаунту на Госуслугах. После этого в личный кабинет могут быть загружены различные поддельные доверенности, заявки, с помощью которых злоумышленники продолжают вводить жертву в заблуждение. Но на этом схема не заканчивается. Далее к разговору подключаются якобы представители различных ведомств, в том числе лжеправоохранители, которые убеждают человека, что его личный кабинет взломан. Цель - под любыми предлогами вынудить граждан осуществить денежные переводы личных средств или взятых в кредит. И перевести их на «безопасный» счет.

Важно запомнить основные правила безопасности:

- если вам поступил звонок от неизвестного, и вам предлагают передать код или речь заходит о ваших деньгах, немедленно прервите разговор! Это мошенники!

- никогда и никому нельзя говорить пароли или коды, присылаемые вам посредством сообщений. Код от вашей карты и пароли подтверждения операции не имеет право запрашивать даже сотрудник банка. Как показывает практика последних дней, если вам пришел код и его спрашивают неизвестные – значит они пытаются получить несанкционированный доступ к вашей странице на портале «Госуслуг».

- не устанавливать на телефон или компьютер программы удаленного доступа, либо включать демонстрацию экрана по просьбе третьих лиц.

- помните: никаких «безопасных» счетов не существует;

- никогда сотрудник Министерства образования, вуза, банка, Роскомнадзора либо правоохранительных органов не позвонит вам по подозрительной операции по вашим счетам;

- если вы все-таки передали код или иные данные, и поняли, что вас обманули, постарайтесь как можно быстрее лично обратиться в ближайший МФЦ и заблокировать возможность входа посторонних лиц в ваш личный кабинет на «Госуслугах».

Расскажите о нашей беседе старшеклассникам и студентам вузов и колледжей. Предупредите их о действиях мошенников. Акцентируйте внимание на том, как они вводят своих жертв в заблуждение.