Городской округ Архангельской области
«Северодвинск»

АДМИНИСТРАЦИЯ СЕВЕРОДВИНСКА

Управление образования

ул. Ломоносова, д. 41а, г. Северодвинск,
Архангельская область, 164507
тел/факс: (8184) 56-15-11
e-mail: gor@edu.severodvinsk.ru

от 14 ОКТ 2020 № 22-01-13/5858

на № _____ от _____

Руководителям подведомственных учреждений и предприятия

О размещении лекционного материала на информационных стендах и официальных сайтах

Уважаемые руководители!

В соответствии с письмом УМВД России по Архангельской области от 02.10.2020 № 26/181 направляем для использования в работе лекционный материал для проведения профилактики дистанционных преступлений и мошенничеств среди сотрудников образовательных организаций.

Просим разместить лекционный материал на информационных стендах и официальных сайтах в срок до 23.10.2020.

Приложение: на 2 л. в 1 экз.

Начальник С.Г. Попа

Шпак Сергей Григорьевич
54 80 90 (доб. 226)

Лекционный материал – профилактика мошенничества

Проблема дистанционных преступлений для нашего региона, как и для всей страны в целом, не теряет своей актуальности. Несмотря на постоянную профилактическую работу, с начала 2020 года количество зарегистрированных случаев телефонного и интернет мошенничества и дистанционных краж с банковских счетов граждан в Архангельской области возросла почти на 75%.

1. Наиболее частым способом совершения преступлений является звонок от лица службы безопасности банка. Потерпевшему сообщают, что с его счета совершена попытка несанкционированного списания денежных средств (вариант – на ваше имя пытаются дистанционно оформить кредит). Для предотвращения операции предлагают продиктовать номера банковской карты и коды безопасности, приходящие в СМС-сообщениях. Эти сведения строго конфиденциальны! После их разглашения преступники получают доступ к вашему банковскому счету!

ЗАПОМНИТЕ! Службы безопасности банков никогда не звонят клиентам с сообщениями о проблемах со счетом. Любой подобный звонок – дело рук мошенников. Все вопросы, связанные с обслуживанием вашей банковской карты необходимо решать только по телефону службы технической поддержки, который расположен на оборотной стороне любой банковской карты. Он бесплатный и круглосуточный. Никогда и никому не сообщайте номера и коды безопасности банковских карт!

2. Покупки в сети Интернет. Чаще всего преступления совершаются с использованием сервисов бесплатных объявлений (авито, юла и т.д.) Причем жертвой преступления может стать как покупатель, так и продавец.

- Так при размещении объявления о продаже вещи человеку поступает звонок от потенциального покупателя. Он сообщает, что готов приобрести данную вещь и предлагает внести предоплату. Для перечисления денег просит сообщить данные банковской карты, включая CVV код и коды безопасности из СМС-сообщений. После передачи конфиденциальных сведений со счета потерпевшего происходит списание денежных средств.

- При покупке вещи в сети интернет необходим помнить, что любой дистанционный перевод денежных средств незнакомому человеку потенциально опасен. Вы не можете гарантировать, что он выполнит свою часть сделки. То же касается и не проверенных интернет-магазинов. Вы можете не получить оплаченную вещь, либо получить совсем не то, что заказывали. Пользуйтесь проверенными сервисами и системами безопасного расчета.

3. Большое число преступлений совершается через социальные сети. Чаще всего страницы пользователей взламываются, либо копируются. После чего кругу «друзей» рассылаются сообщения с просьбой дать денег в долг.

Никогда не перечисляйте деньги после просьб в соцсетях. Обязательно созвонитесь с человеком ЛИЧНО.

4. Еще одна преступная схема – предложения от имени известных банков принять участие в розыгрыше и гарантированно получить денежный приз. Для этого необходимо заполнить специальную форму, куда, помимо персональных сведений, необходимо внести конфиденциальную информацию о номерах и кодах безопасности банковской карты. После разглашения данных конфиденциальных сведений со счета потерпевшего списываются денежные средства.

5. Не устанавливайте на телефон неизвестные мобильные приложения. Среди них могут оказаться как вирусные программы, так и сервисы по удаленному управлению телефоном. Если у вас подключены системы дистанционного управления финансами, данные вредоносные программы получат доступ к ним и к вашим сбережениям. Чтобы обезопасить себя, не переходите по сомнительным ссылкам в СМС и ММС сообщениях, не устанавливайте программы, назначение которых вам не понятно, используйте лицензионное антивирусное программное обеспечение!

Будьте бдительны. Не позволяйте мошенникам обманывать вас.