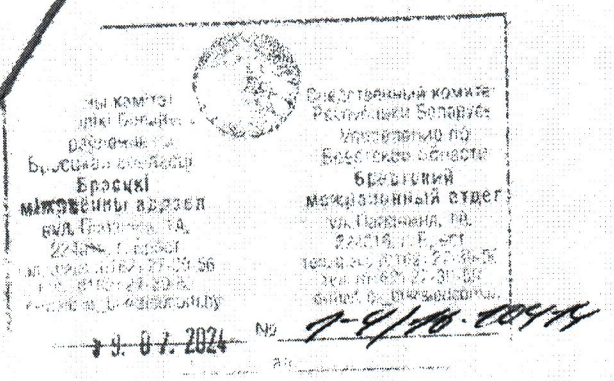


Начальнику главного
управления по образованию
Брестского областного
исполнительного комитета
Калиновской Н.А.

ул. Ленина, 11
224005, г. Брест

Об информировании

Уважаемая Наталья Анатольевна!

Следственным комитетом отмечается рост преступлений, сопровождаемых несанкционированным доступом к учетным записям интернет-мессенджеров и социальных сетей в отношении работников организаций и предприятий.

С целью недопущения совершения данного вида преступлений просим довести до подчиненных сотрудников и подведомственных организаций схему мошенничества «Фейк-босс».

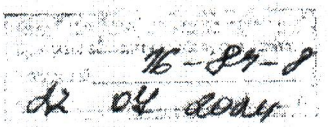
Приложение: на 1 л., в 1 экз.

С уважением,

Начальник отдела А.Н.Вечорко

На электронный!

4 Фунт 8 0162 27 39 38



Следственным комитетом отмечается рост преступлений, сопровождаемых несанкционированным доступом к учетным записям интернет-мессенджеров и социальных сетей в отношении работников организаций и предприятий.

Установлено, что злоумышленники изучают средства обмена сообщениями (данные участников переписки, содержание сообщений в чатах, группах, каналах и личных переписках) в различных мессенджерах и социальных сетях, используемых работниками для коммуникации, определяют учетные записи руководителей, создают копии их учетных записей и вступают в личную переписку с иными участниками таких чатов.

В ходе переписки, выдавая себя за руководителя, злоумышленник сообщает вымышленные сведения о том, что работником интересовались сотрудники правоохранительных органов (называет данные этих «сотрудников») и настаивает на сохранении конфиденциальности факта общения. Указанный психологический прием в ряде случаев снижает уровень критической оценки гражданином последующих действий преступников, обеспечивая беспрекословное выполнение поступающих от них указаний.

Далее гражданину поступают звонки посредством мессенджеров или телефонной связи от якобы сотрудников правоохранительных органов, а также банковских учреждений, в некоторых случаях с демонстрацией посредством мессенджеров фотографии поддельных служебных удостоверений. В ходе беседы псевдосотрудники убеждают в необходимости совершения определенных действий, в том числе по перечислению денежных средств под различными мошенническими предлогами.

Такими предлогами совершения хищений денежных средств могут быть:

- участие в специальной операции по поимке «преступников», которые якобы пытаются похитить деньги с использованием счетов гражданина или от его имени;

- наличие информации о якобы совершении гражданином преступных финансовых операций, для снятия подозрения, в которых необходимо совершить требуемые действия;

- планируемое проведение обыска по месту жительства гражданина с целью выявления и изъятия незадекларированных наличных денежных средств.

Убедив работника в правомочности своих действий, звонящий предлагает передать посреднику наличные денежные средства или внести их на указанные им банковские счета; перечислить денежные средства с банковских счетов, в том числе оформив на свое имя для этих

целей кредиты; предоставить реквизиты своих банковских карт, аутентификационные данные для доступа к банковским счетам, коды из поступивших sms-сообщений и т.д.

В связи с изложенным, просим довести настоящую информацию трудовому коллективу, проинформировать об описанном способе совершения преступлений и рекомендовать им:

- при поступлении подобных сообщений в мессенджерах проверять принадлежность соответствующей учетной записи тому лицу, именем которого учетная запись названа и (или) фотоизображение которого присутствует в профиле (сверить абонентский номер, связаться с владельцем учетной записи по иным каналам связи);

- никому не сообщать реквизиты банковских карт, аутентификационные данные для доступа к банковским счетам, содержание sms-сообщений, поступивших на личные абонентские номера;

- в случае осуществления несанкционированного доступа к учетной записи интернет-мессенджера или социальной сети принимать незамедлительные меры по уведомлению о случившемся граждан, общение с которыми осуществлялось в указанном интернет-мессенджере или социальной сети, с целью предупреждения о возможных попытках осуществления в отношении них преступных действий;

- незамедлительно информировать о выявленных попытках руководство организации (предприятия) для принятия мер по упреждению подобных действий и правоохранительные органы для реагирования.