ПРОФИЛАКТИЧЕСКАЯ АКЦИЯ «КИБЕРДЕТИ»

На территории Республики Беларусь с 23 мая по 1 июня пройдет декада кибербезопасности «КиберДети». В рамках нее организуют комплекс мероприятий, направленный на противодействие киберпреступности и повышение цифровой грамотности учащихся и их родителей, педагогических работников.

В рамках акции пройдут деловые игры, круглые столы и другие мероприятия. Выступать перед адресатами будут сотрудники органов внутренних дел, представители следственных органов, прокуратуры и других силовых ведомств.

Подобные профилактические акции в нашей стране проходят уже не первый год и имеют свои результаты.

О проблеме в цифрах

Согласно статистике, в январе-апреле 2023 г. на территории области зарегистрировано 622 киберпреступления. Большинство зарегистрированных преступлений составляют хищения путем модификации компьютерной информации, причем 88,2% из них совершено без прямого доступа к терминальным устройствам с использованием методик «вишинга» и «фишинга», что создает объективные проблемы по установлению лиц их совершивших. Из 62 преступлений, совершенных с использованием терминальных устройств, расположенных на территории Республики Беларусь (т.н. «бытовых»), на текущий момент раскрыто 88,7%.

Почему и как совершаются преступления?

Условием, способствующим распространению числа имущественных преступлений, учтенных по линии ПК, является широкое распространение различных видов криптовалют и иных цифровых активов, операции с которыми зачастую не поддаются регулированию, в связи с чем на протяжении января-апреля 2023 года велась активная работа по пресечению деятельности лиц, осуществляющих обмен похищенных денежных средств на цифровые знаки.

Правоохранители отмечают, что, учитывая, что основная масса преступлений, регистрируемых по линии киберпреступности, совершается с использованием различных методик социальной инженерии, то такие правонарушения могут совершаться только при условии, когда достаточно большие массы населения не владеют основами цифровой безопасности. Соответственно, доведение правоохранителями этой информации позволяет людям избежать подобных преступлений.

Важно отметить, что информатизация очень быстро распространяется во всех сферах деятельности. Учитывая активность подрастающего поколения и их желание испробовать каждую новинку, они более широко, чем люди старшего возраста, используют компьютерные технологии. Соответственно, во многом то, что им кажется невинной шалостью, на самом деле может образовывать состав преступления.

Какие киберпреступления самые распространенные?

ВИШИНГ

Вишинг – один из методов мошенничества, когда злоумышленники звонят жертве и от имени банковского сотрудника сообщают, что необходимо осуществить какие-либо действия с БПК, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев реквизитами карты, преступники осуществляют хищение денежных средств с банковского счета потерпевшего.

ФИШИНГ

Фиишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

СВАТИНГ

Сватинг – заведомо ложный вызов полиции, аварийно-спасательных служб, путем фальшивых ложных сообщений об опасности (например, о минировании, убийствах, захвате заложников). В последние годы сватинг из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран. Общественная опасность таких деяний состоит в том, что заведомо недостоверные сведения дезорганизуют нормальную работу объектов транспорта, предприятий, государственных органов и учреждений, организаций независимо от формы собственности. В свою очередь, это причиняет существенный экономический вред как субъектам хозяйствования, так и гражданам. При этом информация о возможном взрыве, поджоге либо иных действиях, предполагающих тяжкие последствия, способна посеять панику среди населения и внести неудобства в повседневную жизнь.

ДДОС-атаки

DoS – это атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен. В настоящее время DoS и DDoS-атаки популярны тем, что позволяют довести до отказа практически любую систему.

ГРУМИНГ

Груминг – это вхождение взрослого человека в доверие к ребенку с целью сексуального самоудовлетворения. Злоумышленник дистанционно нащупывает связь с ребенком через социальные сети, мессенджеры, онлайн-игры, электронную почту. Затем может вынудить ребенка прислать фотографии интимного характера, вовлечь в изготовление порнографических материалов, склонить к интимной встрече в реальности.

КИБЕРБУЛЛИНГ

Кибербуллинг – травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди. Эта форма психологического террора может принимать разные обличия: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной

информации о жертве; физическая агрессия и так далее. Причины кибербуллинга: чувство превосходства, зависть, чувство превосходства над соперником, чувство собственной неполноценности, самореализация. Угроза нового времени – так называемые группы смерти. И хотя обычно создателями таких групп являются сами подростки (цель – «хайп», жажда острых ощущений, желание доминировать и управлять другими), в подобных группах создается благоприятствующая атмосфера для культивирования суицидальных намерений.

Как избежать уловок мошенников?

- Не вводите данные карты (особенно - срок действия и CVV-код) на сайтах, куда перешли по ссылкам от незнакомцев. Не соглашайтесь уходить с торговой площадки и продолжать переписку в другом приложении.

- Не переходите ни по каким ссылкам из письма (даже если они якобы ведут к результатам игры). Через поисковик узнайте, действительно ли розыгрыш был проведен, есть ли другие призеры.

Помните, что визуально заметить подмену сложно, но есть характерные маркеры:

- замочек слева от адресной строки не замкнут или есть надпись «Не защищено»;

- электронный адрес ненастоящий или буквы в нем перепутаны (bel-post.by вместо belpost.by, bealrusbank.by вместо belarusbank.by).

- Не переходите по ссылкам на незнакомые ресурсы: с их помощью мошенники пытаются заразить ваш компьютер или телефон вирусом и украсть ваши личные данные.

- Не высылайте денег человеку, с которым вы лично не знакомы, и уж тем более не называйте ему личную информацию, способствующую взлому банковских данных и краже денежных средств.

- Не переходите по ссылкам на незнакомые ресурсы: с их помощью мошенники пытаются заразить ваш компьютер или телефон вирусом и украсть ваши личные данные.

- Если у вас есть сомнения в личности покупателя, лучше созвонитесь с ним, желательно по видеосвязи. Или, если это возможно, предложите личную встречу.

Уважаемые граждане, в любой ситуации необходимо проявлять бдительность и помнить, что абсолютное большинство киберпреступлений становятся возможными ввиду неосмотрительности со стороны пользователя.
Если в отношении вас либо ваших близких совершено противоправное деяние – немедленно сообщите об этом в правоохранительные органы.