**Тезисы лекции по теме:**

**«Профилактика дистанционного мошенничества»**

Цифровая революция в современной реальности способствовала широкому распространению мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий (далее - ИКТ).

В настоящее время насчитывается большое количество современных и разнообразных способов совершения мошенничества в сфере ИКТ. Наиболее распространенные из них:

1. **Фишинг** (от англ. fishing - рыбная ловля) - это вид мошенничества в сети Интернет, когда злоумышленник выдает себя за доверенное лицо, чтобы получить доступ к личной информации пользователя, такой как логины, пароли, данные банковских карт и т.д. Зачастую фишинг осуществляется через поддельные электронные письма, сайты-клонировщики, имитирующие официальные страницы банков, сервисов и других организаций.

2. Мошенничество, совершенное при помощи **онлайн-покупок,** характеризуется тем, что мошенники используют различные схемы, чтобы обмануть пользователей интернет-магазинов и получить денежные средства без отправки товара.

3. **Взлом аккаунта** в одной из социальных сетей. Этот способ, с одной стороны, характеризуется менее подозрительным, поскольку сообщения с финансовой просьбой приходят от знакомого человека, с которым обычно активно ведется или велась переписка. С другой стороны – сложность данного способа заключается в том, что получить способ к чужой интернет-странице требует технических навыков и знаний у мошенника.

4. **Телефонный звонок от лжесотрудников банка или правоохранительных органов** для получения доступ к конфиденциальной информации или убеждения жертвы произвести конкретные действия, которые в дальнейшем привели к финансовым потерям.

5. **Звонок или рассылка SMS о выигрыше приза.** Мошенник сообщает потенциальному потерпевшему информацию о выигрыше определенной суммы денег, туристической путевки или крупной бытовой техники. Если потерпевший поверил, то преступник указывает на необходимость оплатить налог или комиссию для получения «выигранного приза», например, произвести валютную конвертацию.

Для сведения также сообщается, что в настоящее время мошенники стали использовать **нейросети.**

Например, Microsoft VALL-E - это технология, которая использует нейросети для создания голосовых ассистентов, которые могут общаться с людьми на естественном языке. Мошенники могут использовать VALL-E для создания поддельного голосового ассистента от имени легитимной компании или сервиса. Они могут звонить на телефон жертвы и общаться с ней, используя поддельный голосовой ассистент, чтобы запрашивать личную информацию, такую как пароли и номера кредитных карт.

Также мошенники могут использовать поддельный голосовой ассистент в звонке со знакомого номера, чтобы убедить жертву, что он общается с близким человеком и необходимо совершить денежные переводы. Данная технология способна воссоздавать голос человека на основе образца речи продолжительностью в пару секунд.

В силу того, что дистанционные мошеннические действия всегда совершаются с обязательным участием потерпевшего, то меры предупредительного и профилактического характера должны быть, в первую очередь, ориентированы на население.

Для начала каждому необходимо задать себе **следующие вопросы:**

1. Известны ли Вам наиболее популярные способы дистанционных мошеннических схем?

2. Если да, делитесь ли Вы такой информацией со своими близкими, особенно с родственниками пожилого возраста?

3. Ваши учетные записи и личные онлайн-кабинеты защищены двухфакторной аутентификацией? Особенно это касается портала «Госуслуги» и сервисов «Мобильный банк» различных кредитных организаций.

4. Часто ли Вам поступают звонки на телефон с незнакомых номеров? Знаете ли Вы, что у Вашего оператора связи существует защита от спам-звонков? Пользуетесь ли данной услугой?

5. Обладаете ли Вы информацией о том, что сотрудники банковских организаций и правоохранительных органов никогда не осуществляют телефонные звонки гражданам по вопросам кражи Ваших денежных средств со счетов?

Положительные ответы на эти вопросы хотя бы у половины населения нашей страны способствовали бы в какой-то мере более эффективному предупреждению дистанционных мошенничеств.

Помните: важно соблюдать меры кибербезопасности при проведении онлайн-операций, быть бдительными, не передавать свои личные данные и не открывать подозрительные ссылки и файлы!

Прокуратура Московского района г. Калининграда

2025 год