Киберпреступность.

Ситуация с киберпреступностью и кражей денег у населения по телефону с каждым годом лишь ухудшается – власти уже официально признают ее национальной проблемой. Злоумышленники действуют на опережение и находятся на несколько шагов впереди тех, кто им противодействует: законодательство не поспевает за новыми угрозами в сфере высоких технологий и схемами краж денег «сотрудниками безопасности банка». Масштабы киберпреступности достигли таких размеров, что позволяют называть их угрозой национальной безопасности, признавал в мае представитель Генпрокуратуры Андрей Некрасов. При этом раскрывается не более 25% из таких преступлений, отмечал он. [6] К категории киберпреступности относятся, например, такие традиционные преступления, как аферы, мошенничество, вымогательство, шантаж, но совершаемые через интернет и/или с применением вредоносных программ и вычислительных устройств. Киберпреступность, то есть преступления в киберпространстве, быстро стала серьезной мировой проблемой ввиду резкого роста числа пользователей компьютеров, смартфонов и др., а также в связи с тем, что для нее не существует никаких границ, и это существенно затрудняет обнаружение и наказание киберпреступников. [5] Конвенцией Совета Европы виды киберпреступлений объединены в пять групп. Первая группа включает все компьютерные преступления, направленные против компьютерных данных и систем (например, незаконный доступ, вмешательство в данные или системы в целом). Вторую группу составляют противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, получение экономической выгоды иными способами). Правонарушения третьей группы связаны с содержанием данных или контентом. Нарушение авторских и смежных прав относится к четвертой группе. Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность, включаются в пятую группу киберпреступлений. [2] Киберпреступление, как и любое иное преступление, является плодом труда одного или нескольких злоумышленников, в данном случае с обширными знаниями в области Интернета и цифровых технологий, используемыми для достижения корыстных целей. Киберпреступники используют целый арсенал узкоспециальных знаний и навыков в целях получения несанкционированного доступа к банковским счетам, совершения краж личности, вымогательства финансовых средств, мошенничества, преследования и запугивания или использования зараженного компьютера в разветвленной сети ботнетов с целью совершения DDoS-атак на крупные организации. [1] Для защиты от киберпреступников, использующих самые разные технологии, чтобы атаковать компьютеры и получить доступ к пользовательским данным, требуется многоуровневая антивирусная защита. Антивирусы, сочетающие сигнатурный метод, эвристический анализ и облачные технологии, уверенно защищают ваши устройства и ваши данные от новых сложных угроз. [3] Как не стать жертвой киберпреступления:

1. Регулярно обновляйте ПО и операционную систему

2. Установите антивирусное ПО и регулярно его обновляйте

3. Используйте сильные пароли

4. Не открывайте вложения в электронных спам-сообщениях

5. Не нажимайте на ссылки в электронных спам-сообщениях и не сайтах, которым не доверяете

6. Не предоставляйте личную информацию, не убедившись в безопасности канала передачи

7. Свяжитесь напрямую с компанией, если вы получили подозрительный запрос

8. Внимательно проверяйте адреса веб-сайтов, которые вы посещаете

9. Внимательно просматривайте свои банковские выписки [4]

Также, не доверяйте слишком заманчивым предложениям. Такие фразы, как «бесплатно», «почти даром», «подарок», «большие скидки». Мошенники всегда используют эти фразы и хорошо понимают человеческую сущность. Как правило, обещается большая зарплата за минимум труда, большие деньги за небольшое вложение, заем даже если у Вас плохая платежеспособность и так далее. [7]

Список литературы и интернет-ресурсов:

1. avast.ru: сайт. – 2020. – URL: https://www.avast.ru/c-cybercrime

2. internetpolicy.kg: сайт. – 2018. – URL: https://internetpolicy.kg/literacymodule/course_2/module1/glava1_1.html

3. Kaspersky: сайт. – 1997. – URL: https://www.kaspersky.ru/resource-center/threats/cybercrime

4. Kaspersky: сайт. – 1997. – URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime

5. tadviser: сайт. – 2020. – URL:https://www.tadviser.ru/index.php/Статья:Киберпреступность

6. Ведомости: сайт. – 2021. – URL: https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti

7. Следственное управление Следственного комитета Российской Федерации по Самарской области: сайт. – 2020. – URL: https://samara.sledcom.ru/Zashhitim-sebya-ot-kiberprestupnosti