ПРОФИЛАКТИКА ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКОЙ ПЛАТЕЖНОЙ КАРТОЧКИ

Василенок Я.В., курсант уч. гр.9108 ФМОБ

Академия Министерства внутренних дел Республики Беларусь
г. Минск, Республика Беларусь

Сачек А.Г. – канд. юрид. наук, доцент

Аннотация: В статье представлено краткое описание истории развития платежной системы. Охарактеризовано понятие фишинга, описана одна из его новых форм. Составлены рекомендации по безопасным платежам в сети Интернет.

Ключевые слова. Банковская платёжная карточка, фишинг, профилактика, хищение, киберпреступления.

Развитие финансово-кредитной системы привело к увеличению доли безналичных расчетов в экономике. В настоящее время значительное количество граждан Республики Беларусь обращается в правоохранительные органы с заявлением о хищении денежных средств со счетов, к которым выпущены банковские платежные карточки (далее – БПК).

Первая банковская платежная кредитная карточка была выпущена в нью-йоркском районе Бруклин Дж.С. Биггинсом, специалистом по потребительскому кредиту из национального банка «Флэтбуш». В 1946 году Биггинс организовал работу по кредитной схеме под названием Charge-it. От клиентов местными магазинами за мелкие покупки принимались расписки, после покупки магазин сдавал расписки в банк, а банк оплачивал их со счетов покупателей. Впервые была опробована классическая цепочка расчётов.

В 1976 году National BankAmericard Inc. переименовала свою карточку BankAmericard в известную теперь всем Visa, а в 1980 году Card Association дала своей карточке название MasterCard.

В настоящее время существуют несколько международных банковских ассоциаций, карточки которых популярны и обслуживаются в практически во всех уголках мира: Visa International, MasterCard International, Europay International, JCB и Diners Club.

Республика Беларусь стала осуществлять операции с использованием карточек международных банковских ассоциаций начиная со второй половины 1993 года. В марте 1992 года ведущие белорусские банки совместно с Национальным банком Республики Беларусь приступили к созданию национальной системы безналичных расчетов на основе БПК «Белкарт».

Первое разрешение на право осуществления операций с использованием БПК Europay, MasterCard получил Белвнешэкономбанк 8 декабря 1995 года, а с карточками системы «Белкарт» - Беларусбанк 16 января 1996 г. В настоящее время в нашей стране активно развивается платежная система «Мир». В 2020 совместно с платежной системой «Белкарт» была создана БПК «Белкарт-Премиум». Рассчитываться БПК «БЕЛКАРТ-ПРЕМИУМ» можно в сети обслуживания платежной системы «Мир» и ее) систем-партнеров - в Российской Федерации, Армении, Узбекистане, Казахстане, Кыргызстане, Таджикистане, Турции, Вьетнаме. Также существует комбрейдинговая карта «Белкарт-Maestro» сочетающая в себе 2 платёжные системы «Белкарт» и «MasterCard». Обязательная авторизация всех операций с использованием карточки, а также наличие чипа обеспечивает держателям карточек высокую степень сохранности денежных средств и дополнительную безопасность при проведении платежей.

Как отметила, ученая Морозова Е.А. «одним из основных «бедствий» последних лет, связанных с повсеместным распространением кибертехнологий стало кибермошенничество. Обусловлено это высоким уровнем латентности данного вида преступлений, а также существенных трудностей, возникающих в процессе его раскрытия и расследования» [2].

Опасность кибермошенничества определяется недостаточным уровнем их изученности, отсутствием новых методик по их расследованию, незнания способов их совершения, а также мер по их предотвращению, также проблемой является нехваткой квалифицированных IT-специалистов для оказания содействия следственным подразделениям.

Хищение путем использования компьютерной техники возможно лишь посредством компьютерных манипуляций. Компьютерное «хищение» предполагает перехват информации, несанкционированный доступ к средствам информации, проведение манипуляций с данными и управляющими командами. При манипулировании с процессами ввода, вывода информации компьютер, согласно заложенной в него программе, идентифицирует преступника как законного владельца денежных средств или иного имущества. Преступник не сам тайно изымает эти деньги, а компьютер, банкомат, другое электронное устройство передает ему информацию, в которой заложена ошибка. Завладение чужим имуществом в данном случае может происходить путем ввода, изменения, удаления или блокировки компьютерных данных либо путем другого вмешательства в функционирование компьютерной системы.

Как показывает практика, халатное отношение пользователей к хранению своих личных данных является основной причиной обманов, совершаемых в Интернете. Одним из самых распространённых видов цифрового мошенничества является фишинг, суть которого – под любым предлогом узнать конфиденциальную информацию с последующим использованием ее в корыстных целях.

Относительно недавно мошенники разработали новую форму фишинга. Они создают сайты-копии интернет-магазинов, налоговой службы и службы судебных исполнителей, где необходимо производить оплату, а, соответственно, вводить данные реквизиты БПК, а также сайты – копии социальных сетей и иных сервисов, где необходимо производить вход через логин и пароль.

В настоящее время правоохранительные органы ведут активную работу по противодействию рассматриваемым видам преступлений. Однако с точки зрения обеспечения безопасности физического лица единственным способом защиты от цифрового мошенничества включая и фишинг является внимательное отношение к своим персональным данным.

Мы поддерживаем мнение специалистов в сфере цифровой безопасности и считаем, что в качестве наиболее действенных рекомендаций по предупреждению мошенничества в сети Интернет можно выделить следующие:

не заходить на подозрительные ссылки, отправленные незнакомцами;

установить антивирусное ПО на свою компьютерную технику, способное отслеживать нежелательные вложения;

не разглашать в личных переписках даже самым близким родственникам свои данные, потому что нельзя на 100% обезопасить себя от взлома в социальной сети;

установить двухфакторной аутентификации в социальных сетях и электронной почте, подразумевающую получение СМС-сообщения о входе в соответствующий интернет-ресурс.

Список использованных источников:

1. Организация расследования преступлений с сфере высоких технологий: учебное пособие/ П.В.Гридюшко [и др.]; под общ.ред. И.Г.Мухина; учреждение образования «Акад. М-ва внутр.дел Респ. Беларусь». – Минск: Академия МВД,2017.- 139,[1] с.

2. Сабырбаева,А.Б. К некоторым проблемам, возникающим в ходе расследования кибермошеничества [Электронный ресурс/Сабырбаева А.В.//Судебно-правовые реформы: национальный и зарубежный опыт: материалы междунар. Науч.-практ. конф (30 сент. 2021 г.)/ Ун-т обществ. Безопасности Респ. Узбекистан; [отв. Ред. Рустамбаев М.Х., редкол.: Селиманова С.М. и др.], - Ташкент,2021. – Ч.2.- с.15-22. УДК 343.985.7

3. Уголовный кодекс Республик Беларусь: науч-практ. коммент./Т.П. Афонченко [и др.]; под ред. В.М. Хомича, А.В.Баркова, В.В. Марчука. – Минск: Нац.центр правовой информ. Респ. Беларусь,2019. – 1000 с.

4. Белкарт- новая карточка: [Электронный ресурс]// ОАО «АСБ Беларусбанк». URL: https://belarusbank.by/ru/fizicheskim_licam/cards/international/35715 (Дата доступа 05.04.2022).

5. Карточка- «Шчодрая»: [Электронный ресурс]// ОАО «АСБ Беларусбанк». URL: https://belarusbank.by/ru/fizicheskim_licam/cards/32326/33697 (Дата доступа 05.04.2022).

6. Как не стать жертвой фишинга: [Электронный ресурс]// Новости Беларуси|БелТа. URL: https://www.belta.by/infographica/view/kak-ne-stat-zhertvoj-fishinga-24467/ (Дата доступа 05.04.2022).