



Тематическое приложение к газете **Коммерсантъ**

Безопасность

Пятница 19 февраля 2021 №30 (6992 с момента возобновления издания)



perm.kommersant.ru

12 | Когда могут быть сняты ограничения, связанные с COVID-19

В 2020 году разнообразная деятельность в онлайн стала еще более привычной для широкого круга пользователей, при этом выросла активность интернет-мошенников. Киберпреступники переключились с банкоматов и организаций торговли на каналы банковского онлайн-обслуживания, констатируют эксперты. И это результат не «прорех» в системах банковской защиты, а совершенствования криминальных схем. Банкиры и правоохранители регулярно сообщают о необходимости бдительности и алгоритме действий в случае подозрения на мошенничество.

Отпетые кибермошенники

— технологии —

В территориальных органах МВД России по Пермскому краю за 2020 год зарегистрировано 8774 мошенничества и кражи с использованием информационно-телекоммуникационных технологий (рост по сравнению с 2019 годом составил 36,4%). Правоохранители отмечают растущую динамику регистрации киберпреступлений на протяжении последних четырех лет: 1170 случаев в 2017-м, 3415 — в 2018-м, 6431 — в 2019-м, 8774 — в 2020 году.

Отъем с согласия

По данным Банка России, к наиболее распространенным видам дистанционного отъема денег у граждан относится телефонное мошенничество для получения конфиденциальных банковских данных. Как правило, это сообщения или звонки от псевдосотрудников кредитной организации — «служб безопасности» банков, государственных учреждений, официальных организаций. Еще один способ отъема средств — когда жертвы махинаций добровольно предоставляют преступникам конфиденциальную информацию на фишинговых (поддельных) сайтах или сайтах-двойниках, предлагающих товары, псевдофинансовые продукты или услуги, участие в сомнительных финансовых проектах. Кроме того, угрозу представляет внедрение вредоносного программного обеспечения, когда потенциальные жертвы «бродят» по неизвестным интернет-ссылкам и рекламным баннерам, что часто открывает злоумышленникам доступ к конфиденциальным данным и банковским приложениям пользователей.

Отчетность Центробанка по итогам 2020 года пока не опубликована, цифры поквартального подведения результатов таковы. За первые три месяца прошлого года объем операций без согласия клиента вырос на 38% по сравнению с аналогичным периодом 2019 года. Во втором квартале наблюдалось дальнейшее увеличение объема операций без согласия клиента (+59%) на фоне роста общего объема операций с использованием электронного средства платежа. Объем операций без согласия клиентов (доля возмещенных средств) в первом квартале 2020 года в нише банкоматов и терминалов составил 112 млн руб. (плюс 9%), во втором квартале — 127 млн руб. (рост 18%), в третьем — 200,5 млн руб. (рост 6%).

В сфере оплаты товаров и услуг в интернете — в первом квартале объем операций без согласия клиента вырос до 926 млн руб. (плюс 17%) и до 1122 млн руб. (плюс 16%) во втором. В третьем квартале цифра составила 1182,4 млн руб. (плюс 19%).



Мошенник в разговоре с потенциальной жертвой использует приемы психологического воздействия

В части дистанционного банковского обслуживания физлиц — 559 млн руб. (плюс 3%) в первом квартале 2020 года, 728 млн руб. (6%) во втором квартале. В третьем квартале — 944,6 (плюс 5%).

Тренды года

ЦБ сообщил о наиболее распространенных мошеннических схемах и сценариях.

Мошенники «одобрили» моду на QR-коды. Теперь именно в них «зашивают» ссылки на фишинговые сайты, чтобы прислать их продавцам и покупателям на «Авито» и других онлайн-досках объявлений. Злоумышленники зашифровывают фишинговую ссылку в картинку с QR-кодом, чтобы обойти защитные механизмы сайта объявлений. Обычно служба безопасности онлайн-площадки блокирует сомнительные ссылки, но публикацию картинок не запрещает, так как пользователям нужно обмениваться фотографиями товаров.

Нередко мошенники предлагают перенести обсуждение деталей сдел-

ки в сторонний мессенджер — и там могут прислать ссылку или QR-код для перехода на фейковую страницу. На фишинговый сайт могут попытаться увести как покупателя, так и продавца, которому на карту должны поступить деньги.

Не осталась без внимания хакеров актуальная во время самоизоляции тема реструктуризации кредитов. Чтобы вызвать у людей больше доверия, преступники разработали многоступенчатую схему для выманивания денег, в которой фигурируют не только службы безопасности банков, но и бюро кредитных историй (БКИ). Сначала мошенник звонит клиенту от имени сотрудника БКИ и говорит, что несколько банков якобы запросили его историю перед выдачей кредита. Поскольку человек отрицает, что подавал заявки в банки, его наводят на мысль, что кто-то другой пытается взять кредит от его имени по поддельному паспорту.

Затем аферисты предупреждают о том, что передадут информацию о попытке подлога в банки и просят дождаться звонка от банковской службы безопасности. Через пару минут звонит «сотрудник банка» и подтверждает, что «преступники пытались оформить кредит» на имя этого че-

ловека. Чтобы «противостоять злоумышленникам», человека убеждают совершить зеркальные действия — подать онлайн-заявку на кредит, а затем перевести деньги на «безопасный счет», на самом деле — мошеннический. В итоге человек оформляет онлайн-кредит и остается без заемных денег.

Массовый выход на фондовый рынок — еще один «подарок» для мошенников: аферисты создают псевдоинвестиционные компании и обзванивают людей с предложением вложиться в акции неизвестных организаций, которые якобы должны в ближайшее время резко вырасти в цене (если же бумаги не подорожают, то организация-эмитент обещает выкупить их обратно с доплатой). На самом деле такие фирмы ничего не производят, никаких активов у них нет — так что ни заработать, ни вернуть вложенное не получится. Организация-эмитент и псевдоинвестиционная компания, хотя и зарегистрированы как разные юридические лица, часто имеют одних и тех же владельцев. Такая сложная схема призвана запутать людей, которые еще не очень хорошо разбираются в том, как работает фондовый рынок. Поэтому начинающим инвесторам в

Банке России советуют приобретать ценные бумаги только на бирже. Инвестировать только через брокеров или доверительных управляющих, имеющих лицензию ЦБ, а также слушать рекомендации по выбору ценных бумаг только инвестиционных советников, входящих в государственный реестр.

В период пандемии также стали популярными предложения от мошенников о различных компенсационных выплатах и страховых возмещениях, возвратах за непополненные туристические услуги (с предварительной оплатой жертвой комиссий или сообщением для получения выписки и переводов данных своей банковской карты). Кроме того — о псевдостраховых услугах, штрафах за несоблюдение карантинных мер и даже сборах на разработку вакцины.

«Рост количества зарегистрированных преступлений в сфере информационно-коммуникационных технологий обусловлен активно развивающимся применением интернет-технологий, востребованным поведением потерпевших, постоянным возникновением новых способов совершения противоправных деяний, имеющимися возможностями для обеспечения анонимности преступ-

ников, а также необходимостью совершенствования механизмов противодействия им», — предупреждает пресс-служба краевого УВД.

По данным правоохранителей, основная масса зарегистрированных в 2020 году в регионе имущественных преступлений, совершенных с использованием компьютерных технологий, приходилась на мошенничество (5306, или 60,5%). Краж зарегистрировано 3468 (39,5%). Общий ущерб от краж и мошенничеств за прошлый год составил более 623 тыс. руб.

Без паники

Количество мошеннических операций, фиксируемых банками, растет пропорционально увеличению численности обслуживаемых клиентов и количеству клиентских операций, делают вывод участники рынка. Однако общий объем ущерба остается примерно на одном и том же уровне. Таким образом, можно считать, что в целом ситуация не изменилась, резюмирует управляющий банком «Открытие» в Пермском крае Валентина Жильцова. По ее словам, попытки хакерских атак на информационные системы и сервисы банков, как правило, не приводят к серьезным последствиям, по-

Цифровая модель безопасности

В филиале «ПМУ» АО «ОХК «УРАЛХИМ» внедрена инновационная система «ТОХИ+Прогноз» для цифрового моделирования возможных вариантов развития событий в случае нештатных ситуаций на производственном оборудовании. Она помогает диспетчеру предприятия очень быстро и точно спрогнозировать развитие ситуации в случае инцидента и сформировать алгоритм действий для минимизации рисков. Это передовой опыт в химической отрасли России.

На технологическом оборудовании производственных цехов установлены газоанализаторы. Данные с них в экстренных случаях сразу передаются в программный комплекс «ТОХИ+Прогноз». В режиме реального времени он сигнализирует диспетчеру о возникшей опасности, менее чем за минуту производит расчет масштабов инцидента и отображает на мониторе компьютера план предприятия с указанием места возникновения нештатной ситуации и количества людей, которые могут оказаться в зоне эвакуации. Эту же картину оперативно смогут увидеть и должностные лица предприятия, к рабочим местам которых подключена трансляция с монитора диспетчера.

Алексей Аверьянов, директор филиала «ПМУ» АО «ОХК «УРАЛХИМ» в г. Перми:

— Благодаря новому программному комплексу диспетчер сможет очень быстро и наглядно получить информацию о месте и масштабах инцидента, сориентироваться в возникшей ситуации и предпринять правильные неотложные действия. Данный проект является одним из целенаправленных шагов в рамках общей стратегии повышения безопасности работников, принятой в компании «УРАЛХИМ».



Установка системы «ТОХИ+Прогноз» на «ПМУ» — первый опыт внедрения такого программного комплекса не только в холдинге «УРАЛХИМ», но и среди предприятий химической отрасли России в целом. Однако уже сейчас аналогичный проект реализуется в филиале «Азот». Благодаря полученному на «ПМУ» опыту процесс пройдет быстрее и эффективнее.

ЭКСПЕРТИЗА
зданий и сооружений

ГРАНДТЭОН
экспертно-оценочная компания

+7(342)257-03-29

- техническое обследование
- пожарная безопасность
- строительная лаборатория
- инженерные изыскания
- проектирование

<https://gt-59.ru>

