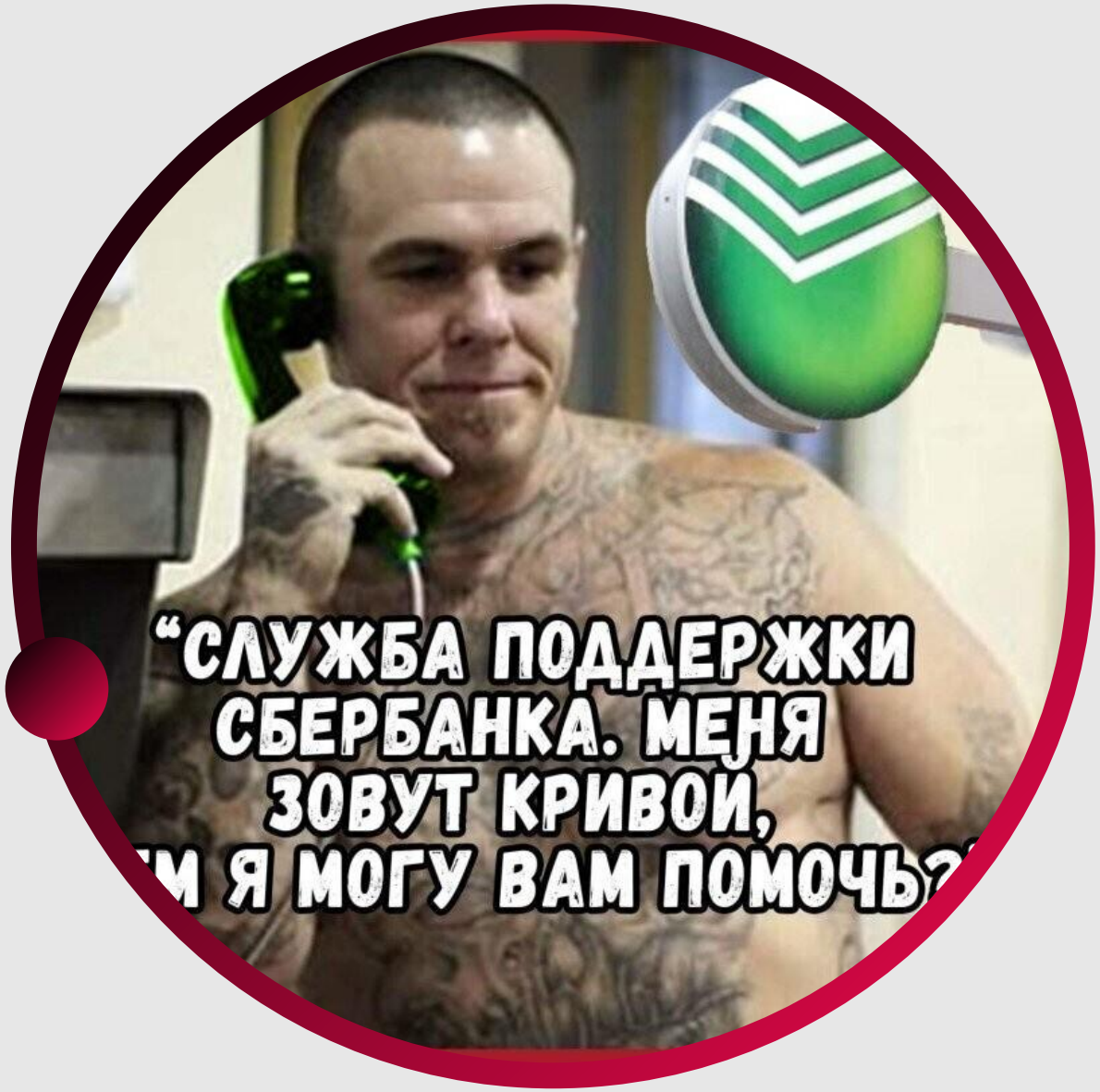

Киберпреступность

ФИШИНГ



Фишинговые электронные письма обычно составляются таким образом, чтобы быть похожими на официальные имейлы от различных финансовых учреждений, налоговой службы или других организаций с целью обманом заставить людей предоставить свою личную информацию.

Фишинг – это один из наиболее распространенных способов кражи личной информации пользователей. Фишинговые практики обычно состоят в том, что киберпреступники притворяются законными представителями той или иной организации, чтобы получить конфиденциальные данные жертв, такие как пароли и номера кредитных карт.

ВЗЛОМ

Хакеры могут даже разрушить репутацию компании, опубликовав конфиденциальную информацию о ней. Порой их называют хактивистами (англ. «hacktivists»). Существует 3 типа хакеров: белая шляпа, черная шляпа и серая шляпа.

Хакинг – это акт получения несанкционированного доступа к компьютерной системе с целью заражения ПК жертвы или обхода мер безопасности. Хакеры – это те, кто используют свои знания для обнаружения уязвимостей в компьютерной системе. Как итог, компании могут столкнуться с различными проблемами (начиная со взлома компьютерной системы и заканчивая получением доступа к конфиденциальным данным).

ПРОГРАММЫ-ВЫМОГАТЕЛИ

Программа-вымогатель – это разновидность вредоносного ПО, которое атакует компьютерные системы, блокирует данные и требует оплаты за их разблокировку. Как только компьютер заражен программой-вымогателем, пользователю предлагается заплатить выкуп, чтобы получить ключ дешифрования, необходимый для восстановления контроля над данными.

Средняя стоимость атаки с использованием программы-вымогателя составляет более 4 миллионов долларов, в то время как деструктивная атака в среднем превышает 5 миллионов долларов. Заражение программами-вымогателями часто можно предотвратить, соблюдая основные правила безопасности, такие как обновление операционной системы или отказ от перехода по подозрительным ссылкам или вложениям от неизвестных отправителей

КРАЖА ЛИЧНОСТИ

Кража личности – это тип киберпреступления, при котором человек использует чужие личные данные, такие как имя и номер социального страхования, номер банковского счета и информацию о кредитной карте, для совершения мошенничества. Плохие «актеры» могут запятнать хорошую репутацию жертвы и испортить ее кредитную историю.

Хакеры собирают информацию о пользователях различными методами, включая взлом компьютера, кражу почты, камеры для захвата данных с экранов ПК и создание поддельных копий удостоверений личности ничего не подозревающих жертв. Затем киберпреступники используют эту информацию, чтобы выдавать себя за жертв, подавать заявки на получение займов, брать под контроль финансы людей, получая доступ к их банковским счетам.

КАК КАРАЮТСЯ КИБЕРПРЕСТУПЛЕНИЯ?

Уголовно-наказуемым является создание, распространение и/или использование компьютерной информации, заведомо предназначенных для неправомерного воздействия на информационную инфраструктуру Российской Федерации. За совершение указанных действий предусмотрено наказание в виде принудительных работ на срок до 5 лет с ограничением свободы, либо лишением свободы на срок от 2 до 5 лет со штрафом от 500 тыс. рублей до 1 млн.

Глава 28 УК РФ. Преступления в сфере компьютерной информации.

- ст. 272 «Неправомерный доступ к компьютерной информации»
- ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»
- ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»
- ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Телефонные мошенники сумели похитить у россиянки 400 млн рублей, что стало самой крупной кражей такого рода за всю историю наблюдений

Ситуация имела место в 2020 году, ее героиней стала женщина 64 лет. Мошенники позвонили ей и представились сотрудниками службы безопасности банка, где у дамы был счет; они сообщили, что ее деньги «нужно спасать» (от чего и зачем – не уточняется). В итоге клиентка банка – к слову, это был не Сбер, а другой крупный банк – сняла со счета 14 млн рублей и перевела их злоумышленникам.

Однако на этом история не закончилась: женщина сообщила мошенникам, что у нее есть еще 380 млн рублей на счетах в других банках. Воры отметили, что эта сумма слишком серьезна, и поэтому ситуацией будет заниматься «сотрудник ФСБ». Последний – естественно, это был никакой не силовик, а соучастник преступления – связался с женщиной и «развел» ее на эти самые 380 млн. В течение месяца она по частям снимала деньги и переводила их туда, куда ей сообщили.

Парам-парам-пам

ВСЁ!