№32 (19576)
ЧЕТВЕРГ 20 АВГУСТА 2026 ГОДА
ГОРОД КОРОЛЁВ • ГАЗЕТА «КАЛИНИНГРАДСКАЯ ПРАВДА»
КАЛИНИНГРАДКА

ОСТОРОЖНО: ЦИФРОВОЙ МИР!

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ

Стремительное развитие информационно-телекоммуникационных технологий (ИТТ) открыло перед человечеством безграничные возможности для общения, работы и творчества. Однако у каждой медали есть обратная сторона: виртуальное пространство стало благодатной почвой для злоумышленников, которые совершенствуют свои методы с каждым днём. Преступления в сфере ИТТ — от банального мошенничества с банковскими картами до сложных хакерских атак — наносят серьёзный ущерб как отдельным гражданам, так и экономике в целом. Именно поэтому профилактика и осведомлённость населения выходят на первый план. Лучший способ борьбы с киберпреступлением — не позволить ему произойти.

ПОРТРЕТ СОВРЕМЕННОЙ УГРОЗЫ

Киберпреступность давно перестала быть уделом одиночек-энтузиастов. Сегодня этим занимаются организованные группы, использующие психологию, социальную инженерию и технические уязвимости. Самые распространённые схемы обмана можно разделить на несколько категорий.

ФИШИНГ (ЛОВЛЯ НА УДОЧКУ) И «ПОДДЕЛЬНЫЕ САЙТЫ»

Злоумышленники создают копии известных интернет-магазинов, банковских порталов или социальных сетей. Жертва, не заметив подмены адреса, вводит логин, пароль или данные карты, которые тут же попадают в руки преступников. Распространяются такие ссылки через электронную почту, СМС и мессенджеры — часто с тревожными заголовками вроде «Ваш аккаунт заблокирован» или «Срочно подтвердите данные».

Пример: вам приходит письмо «от банка» с просьбой обновить данные, вы переходите по ссылке, попадаете на сайт-двойник и сами отдаёте мошенникам ключ к своим деньгам. Отдельно стоит выделить вишинг (мошенничества с использованием голосовой связи: телефонные звонки, автообзвон или голосовые сообщения) и смишинг (мошенничества с использованием поддельных сообщений (СМС, писем, сообщений в мессенджерах): в первом случае звонят якобы из банка или госорганов, во втором — присылают сообщение со ссылкой на вредоносный сайт или просьбой перезвонить на платный номер.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Классика жанра — звонок от «сотрудника службы безопасности банка». Под предлогом блокировки подозрительной транзакции или оформления кредита у жертвы выманивают номер карты, CVV-код, код из СМС или убеждают перевести деньги на «безопасный счёт». Используются и сценарии с «попавшим в беду родственником» или «выигрышем в лотерею». Преступники умело имитируют голоса, подделывают номера телефонов, создают фон колл-центра и давят на страх потери сбережений. Иногда звонят через мессенджеры, представляясь сотрудниками правоохранительных органов или Центробанка.

МОШЕННИЧЕСТВО НА ОНЛАЙН-ПЛОЩАДКАХ

Обман при купле-продаже товаров через сайты объявлений: предоплата за несуществующий товар, отправка фишинговой ссылки для «получения денег», использование поддельных сервисов доставки. Часто злоумышленник предлагает перевести общение в мессенджер, уводит с официальной площадки и там выманивает данные карты или предоплату.

В последнее время распространилась схема с «безопасной сделкой» через фальшивый сайт-посредник, который имитирует популярные сервисы.

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Вирусы-шифровальщики, программы-шпионы и «трояны» маскируются под легальные приложения, документы или ссылки. Они могут незаметно собирать личные данные, пароли, делать скриншоты экрана или полностью блокировать устройство с требованием выкупа.

Заражение часто происходит при скачивании файлов из непроверенных источников, открытии вложений в фишинговых письмах или установке приложений из сторонних магазинов. Опасны также поддельные QR-коды, размещаемые в общественных местах: сканируя их, вы можете перейти на вредоносный ресурс.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Самый опасный и эффективный инструмент. Преступники давят на эмоции: страх, жадность, любопытство, желание помочь. Они торопят, запрещают советоваться с близкими, создают иллюзию срочности. Помните: ни одна настоящая организация не будет требовать мгновенных решений и секретных данных по телефону.

Мошенники часто используют информацию из открытых источников (соцсетей, утечек баз данных), чтобы завоевать доверие: называют ваше имя, должность, адрес.

КАК ЗАЩИТИТЬ СЕБЯ: ПРАКТИЧЕСКИЕ СОВЕТЫ

Предотвратить преступление всегда лучше, чем попытка вернуть украденное. Внедрите в повседневную жизнь несколько простых правил цифровой гигиены — и вы значительно снизите риск стать жертвой.

1. Берегите конфиденциальную информацию как зеницу ока. Никогда и никому не сообщайте полные реквизиты банковской карты (особенно CVV/CVC-код на обратной стороне), коды из СМС и push-уведомлений, логины и пароли от личных кабинетов. Сотрудники банков, государственных органов и технической поддержки никогда не запрашивают эти данные. Если собеседник настаивает — это мошенник. Для онлайн-платежей заведите отдельную карту с ограниченным лимитом и не храните на ней крупные суммы.

2. Создавайте надёжные пароли и используйте двухфакторную аутентификацию. Для каждого важного сервиса (почта, банк, госуслуги) должен быть уникальный пароль длиной не менее 10—12 символов, содержащий буквы в разном регистре, цифры и спецсимволы. Не используйте даты рождения, имена питомцев или простые последовательности. Подключите двухфакторную аутентификацию (вход по коду из СМС или приложению-генератору) — даже если пароль украдут, злоумышленник не сможет войти без второго фактора. Периодически меняйте пароли, особенно если были подозрения на взлом.

3. Будьте «параноиком» в отношении ссылок и вложений. Прежде чем кликнуть по ссылке, наведите курсор и проверьте адрес. Малейшее отличие (например, «sberbank-online.ru» вместо «sberbank.ru», или «gosuslugi.net» вместо «gosuslugi.ru») — повод закрыть страницу. Не открывайте вложения в письмах от незнакомых отправителей, даже если тема кажется важной. Лучше позвоните отправителю и уточните, действительно ли он отправлял файл. Остерегайтесь сокращённых ссылок (bit.ly и подобных) — они могут скрывать фишинговый адрес.

4. Совершайте покупки только на проверенных площадках. При онлайн-шопинге обращайте внимание на наличие значка безопасного соединения (замок в адресной строке) и протокола https. Не переходите по ссылкам из рекламных рассылок — лучше вручную наберите адрес известного магазина в браузере. Для покупок на сайтах частных объявлений используйте только встроенные системы безопасных сделок, никогда не вносите предоплату на карту физического лица и не сообщайте данные карты для «получения перевода». Если продавец торопит и предлагает уйти в мессенджер — это подозрительно.

5. Установите антивирус и регулярно обновляйте программное обеспечение. Современные антивирусные программы способны блокировать фишинговые сайты, вредоносные загрузки и подозрительные действия приложений. Не игнорируйте обновления операционной системы и программ — в них часто уже прописана блокировка обнаруженных уязвимостей. Скачивайте приложения только из официальных магазинов (RuStore, App Store, Google Play), проверяйте название разработчика и отзывы.

6. Настройте приватность в социальных сетях. Не публикуйте избыточную информацию: домашний адрес, номер телефона, геолокацию в реальном времени, фотографии дорогих покупок, планы поездок. Эти данные могут быть использованы для адресного мошенничества (например, звонок «ваш сын попал в аварию, нужны деньги» будет звучать убедительнее, если преступник знает имя и обстоятельства). Ограничьте круг лиц, которые видят ваши публикации.

7. Разговаривайте с пожилыми родственниками. Люди старшего поколения — самая уязвимая группа. Объясните им основные схемы обмана, попросите никогда не сообщать данные карты по телефону, не переводить деньги незнакомцам и обязательно советоваться с вами при любых подозрительных звонках. Установите на их смартфоны определители номеров, блокирующие спам. Научите их проверять информацию: пусть звонят вам или в организацию по официальному номеру.

8. Доверяйте, но проверяйте. Если вам звонят из «банка» и сообщают о проблеме, положите трубку и перезвоните по официальному номеру, указанному на обратной стороне карты или сайте организации. Если «сотрудник полиции» требует перевести деньги для освобождения родственника от ответственности — позвоните самому родственнику. Если покупатель на сайте объявлений предлагает оформить «безопасную сделку» через неизвестный сервис — откажитесь. Помните: настоящие сотрудники никогда не будут возражать против того, чтобы вы перезвонили сами.

9. Регулярно проверяйте банковские выписки. Просматривайте историю операций хотя бы раз в неделю. При обнаружении незнакомых списаний немедленно блокируйте карту и обращайтесь в банк. Подключите СМС-уведомления о всех операциях — это позволит быстро заметить подозрительную активность.

10. Будьте осторожны с публичным Wi-Fi. Не совершайте финансовые операции и не вводите пароли при подключении к открытым сетям в кафе, торговых центрах, аэропортах. Злоумышленники могут перехватывать трафик через поддельные точки доступа. Если необходимо выйти в интернет, используйте мобильный интернет.

11. Регулярно делайте резервные копии данных. Вирусы-шифровальщики могут уничтожить важные файлы. Настройте автоматическое резервное копирование на внешний диск или в облако. Это не защитит от кражи данных, но позволит восстановить информацию без уплаты выкупа.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ВСЁ ЖЕ ПОСТРАДАЛИ?

Если вы поняли, что стали жертвой киберпреступников, действуйте быстро и без паники:

1. Заблокируйте скомпрометированные счета и карты. Позвоните в банк, объясните ситуацию, попросите приостановить операции и оспорить мошеннические транзакции.

2. Смените пароли от всех важных сервисов, особенно от электронной почты и онлайн-банка. Если взломан аккаунт, восстановите доступ через службу поддержки.

3. Сохраните доказательства: скриншоты переписок, номера телефонов, ссылки, квитанции о переводах, записи разговоров (если есть).

4. Обратитесь в полицию. Напишите заявление в ближайшем отделении или через официальный сайт МВД. Чем быстрее вы это сделаете, тем выше шанс вернуть деньги и поймать преступников.

5. Сообщите в банк-получатель. Если вы перевели деньги на карту мошенника, можно попробовать связаться с банком получателя и сообщить о мошенничестве.

6. Проверьте устройства антивирусом. Если вы переходили по подозрительным ссылкам или скачивали файлы, проведите полное сканирование.

Киберпространство — это та же улица, только с более хитрыми карманниками. Соблюдение простых правил безопасности, критическое мышление и здоровая доля недоверия к неожиданным звонкам и сообщениям — ваша главная защита. Помните: преступник рассчитывает на вашу растерянность, доверчивость и спешку. Остановитесь, подумайте, проверьте информацию — и вы не оставите ему ни единого шанса. Берегите себя и свои данные!

ПРОКУРАТУРА ГОРОДА КОРОЛЁВА