Интернет-банкинг без риска: как защитить свои деньги онлайн

Интернет-банкинг давно стал неотъемлемой частью нашей жизни — переводы, оплата услуг, кредиты и инвестиции теперь доступны всего в несколько касаний. Но вместе с удобством вырос и уровень риска: уровень кибермошенничеств в Казахстане растет с каждым годом, а схемы становятся все изощреннее. Чтобы сохранить свои деньги и данные в безопасности, важно знать простые, но жизненно необходимые правила цифровой гигиены.

Соблюдайте базовую цифровую гигиену

Мошенники любят звонить потенциальным жертвам, представляясь сотрудниками банка, а на самом деле выманивают данные, чтобы дальше снять деньги со счета или использовать полученную информацию. Поэтому никому не сообщайте коды из SMS и пароли и не устанавливайте ПО удаленного доступа (AnyDesk/TeamViewer) по просьбе «банка».

Это типичное мошенничество: аферисты через программы получают полный доступ к устройствам и оформляют кредиты, снимают деньги и совершают переводы. Например, в области Жетысу мошенники входили в доверие к гражданам и принуждали их устанавливать на смартфоны приложение AnyDesk. От этой ОПГ пострадали более 40 человек, а общая сумма ущерба превысила 70 миллионов тенге.

Обязательно включите push-уведомления и установите лимиты по операциям. Так вы всегда будете в курсе всех действий, что происходят с вашим счетом, и сразу заметите подозрительные операции.

Используйте только официальные приложения банков и проверяйте адреса сайтов. В противном случае вы можете попасть на «сайт-перехватчик», который украдет ваши данные. Приложения скачивайте только через маркетплейсы App Store и Google Play, а при переходе на сайт проверяйте адресную строку: там должно быть https, а не http, потому что s — secure.

Если вам звонит «сотрудник банка» и давит на вас срочностью или вынуждает перевести деньги на «безопасный счет», то сразу кладите трубку и перезванивайте в банк по официальному номеру.

Защищайте свои устройства всеми возможными способами

Злоумышленники нередко используют такой вид мошенничества как SIM Swapping или SIM Swap — вид атаки, при котором преступники получают у сотового оператора новую SIM-карту с номером жертвы и действуют от ее имени. Чтобы такого не случилось, запросите у мобильного оператора дополнительные меры безопасности, чтобы защитить свой номер. И старайтесь не делиться своим номером в социальных сетях — если это необходимо для работы, то заведите отдельную SIM-карту, через которую не проходят никакие финансовые операции и которая не привязана к важным приложениям.

Помимо номера, защитите свой телефон: установите PIN/биометрию для входа в банковское приложение, блокируйте установки из неизвестных источников, регулярно обновляйте программное обеспечение и антивирус.

Используйте для онлайн-покупок отдельную карту и привяжите к ней отдельный номер. Пусть на этом счету будет небольшое количество денег, нужных для покупок. А на основную карту обязательно ставьте лимиты на онлайн-оплату и переводы.

Старайтесь не использовать публичный Wi-Fi — через него мошенники могут перехватывать данные. Но если вдруг вам срочно нужен интернет, а мобильные данные не работают, то старайтесь не заходить в банковские приложения.

Запоминайте основные признаки мошенничества

Мошенники чаще всего звонят от имени банков, полиции, Генпрокуратуры, КНБ или Казпочты, и просят назвать код/пароль, «подтвердить вход» голосом, установить AnyDesk или «срочно перевести на безопасный счет». Настоящие сотрудники этих структур никогда такого не просят.

Далее, аферисты очень любят торопить и давить на эмоции либо угрожать. Они пользуются вашей растерянностью, чтобы вы сделали все так, как надо им. Как только почувствуете, что на вас давят и вам неприятно — кладите трубку и перезванивайте сами по официальному номеру, чтобы уточнить информацию.

Остерегайтесь массовых фишинговых атак и рассылок: мошенники могут присылать вам ссылку на «оплату штрафа», просить обновить анкету в банке или сообщить, что вы победили в лотерее, но нужно оплатить некий взнос. Все это — мошенничество. Как только перейдете по ссылке или введете личную информацию, аферисты получат доступ к вашим деньгам и персональным данным.

Что делать, если заметили подозрительную активность со своим счетом

1. Сразу блокируйте карты и сообщайте в банк, а потом пишите заявление в полицию.
2. В банковском приложении измените пароль, PIN-код, а потом выйдите из приложения.
3. Соберите доказательства (скриншоты SMS, звонков, ссылок), чтобы приложить их к заявлению в полицию.

Краткий чек-лист

10 полезных советов по защите от мошенничества с интернет-банкингом:

4. Никому не говорите коды, пароли, CVV/CMC-коды банковских карт и не устанавливайте на свои устройства программы удаленного доступа. И лучше вообще ничего не устанавливайте по чужой наводке.
5. Перезванивайте в банк сами по номеру с сайта — не разговаривайте с «сотрудниками», которые просят вас что-то сделать.
6. Включите push-уведомления и установите лимиты, заведите для онлайн-покупок отдельную карту с небольшой суммой.
7. Проверяйте ссылку/домен, а в сомнительных рассылках не вводите данные карты.
8. Защитите SIM от перевыпуска, защитите смартфон кодами, биометрией и антивирусом.
9. Не пользуйтесь интернет-банкингом через публичный Wi-Fi.
10. Регулярно проверяйте кредитную историю.
11. Подключите услугу «Стоп кредит» в eGov/eGov Mobile.
12. При подозрительной активности немедленно блокируйте карты.
13. Подавайте заявления в полицию — либо в отделении, либо через eOtinish, прилагайте к нему все доказательства (скрины, SMS, номера звонков).

Материал подготовлен при помощи www.fingramota.kz