

# Основные виды мошенничеств и их профилактика

## Фишинг

Фишинг – вид интернет-мошенничества, цель которого получить идентификационные данные пользователей (логины и пароли, секретные ключи, номера пластиковых карт и ПИН-коды). Обычно организаторы так называемых фишинг-атак используют массовые рассылки на электронные адреса от имени Банка. В этих письмах может содержаться ссылка на фальшивый сайт, который может выглядеть точь-в-точь как сайт Банка. Вводя свои логин и пароль на этом сайте, вы отдаете их злоумышленнику. В письмах может содержаться просьба от лица Банка (например, от лица администратора системы Интернет-банк) прислать логин, пароль или другую вашу конфиденциальную информацию.

**Банк никогда не запрашивает по электронной почте конфиденциальную информацию Клиентов!**

## Меры профилактики

- проверять адрес Интернет-банка в адресной строке браузера, он должен быть таким: <https://ibank.aibank.ru>
- при обнаружении подозрительного письма незамедлительно сообщить об этом администратору Системы, позвонив по телефону (495) 780-54-59. Подозрительное письмо перешлите в Банк на адрес [support@aibank.ru](mailto:support@aibank.ru) для подробного анализа;
- ни при каких условиях не сообщайте информацию о вашем пароле никому, включая сотрудников Банка. Сотрудники Банка никогда не просят сообщить пароль или выслать секретные ключи;
- не отвечайте на письма, содержание которых вам кажется подозрительным.

## Вредоносные программы

На сегодняшний день существует ряд вредоносных программ, объединенных в несколько классов. Основными классами вредоносных программ являются вирусы, трояны и кейлогеры.

**Компьютерный вирус** – вредоносная программа способная к размножению. Вирус может повреждать или уничтожать информацию или воровать её и передавать злоумышленнику.

**Троянская программа** (также — **троян**) – программа, используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблагоприятных целях.

**Кейлогер** – вредоносная программа, которая позволяет записывать все нажатия клавиш на клавиатуре и, соответственно, все пароли, логины, переписку и т.д.

Заражение вредоносной программой может привести к:

- потере всех информации и соответственно невозможности использования системы Интернет-банк;
- похищению злоумышленником ваших логинов, паролей и секретных ключей и в последствии похищение им ваших денежных средств со счета в Банке.

## Меры профилактики

Для профилактики заражения вредоносной программой стоит придерживаться следующих правил:

- устанавливать все обновления безопасности операционной системы Windows;

- установить и использовать антивирусную программу, регулярно обновлять антивирусную базу. Рекомендуется использовать программные решения ведущих производителей;
- установить и использовать персональный бранмауэр (программа, предотвращающая доступ к данным на вашем компьютере извне). Рекомендуется использовать программные решения ведущих производителей;
- никогда не открывать вложения в письмах от неизвестных отправителей;
- при работе в сети интернет будьте бдительны, устанавливайте дополнительные приложения, только если вы доверяете их разработчику.