Рекомендации о необходимых действиях в период повышенного уровня угрозы проведения компьютерных атак

В современных реалиях достаточно легко потерять денежные средства со своих счетов, если не учитывать в работе меры предосторожности, которые скорее всего уже известны всем клиентам банков. На сегодняшний день из СМИ мы постоянно узнаем, что существует угроза потери денежных средств посредством компьютерных атак.

Поэтому мы хотим еще раз напомнить о крайне важных рекомендациях, которыми не стоит пренебрегать:

1) На автоматизированном рабочем месте (далее – АРМ) (или мобильном устройстве) при работе с системами дистанционного банковского обслуживания (далее – ДБО) рекомендуется устанавливать последние обновления операционной системы;
2) На АРМ (или мобильном устройстве) при работе с ДБО рекомендуется установить лицензионное антивирусное программное обеспечение с последними обновлениями, иметь установленный межсетевой экран для блокировки подозрительного трафика;
3) Использовать в качестве АРМ (или мобильное устройство) при работе с ДБО только один определенный АРМ (или мобильное устройство), доступ к которому есть только у Вас;
4) Держать в тайне все пароли, используемые для входа в систему ДБО (а также реквизиты платежных

банковских карт), при компрометации сразу же обращаться в Банк;

5) При использовании ключевых носителей необходимо хранить их в надежном месте (к примеру, сейф), во время отсутствия опечатывать с помощью защитных одноразовых пломб;
6) Не устанавливать на АРМ (или мобильное устройство) программы удаленного доступа;
7) Не использовать АРМ (или мобильное устройство) для установки игр или приложений развлекательного и т.п. характера, особенно с недоверенных источников;
8) Работать на АРМ, имеющий доступ к ДБО, используя права обычного пользователя (снижает риск заражения);
9) Не переходить по ссылкам в письмах / не открывать вложения писем, которые не ждете во избежание заражения вирусным программным обеспечением;
10) Держать в закладках официальный сайт Банка (или системы ДБО), так как даже в поисковой системе можно случайно пройти на фишинговый (поддельный) сайт, домен которого будет отличаться только на одну букву/цифру.

С полным списком мер по защите можно ознакомиться на сайте Банка - https://www.kamkombank.ru/rus/corporate-customers/remote-service-k/client-bank/ в разделе «Условия предоставления и осуществления электронного документооборота в системе дистанционного банковского обслуживания "Интернет-Банк" для юридических лиц и индивидуальных предпринимателей», а также на сайте https://elf.faktura.ru/elf/app/main?main=pub&pubSection=security