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

1. Совершайте операции в сети Интернет только с использованием протокола 3D Secure (подтверждение операций с использованием одноразового кода).
2. Контролируйте обеспечение невозможности подключения неучтенных съемных машинных носителей информации и мобильных устройств.
3. Остерегайтесь наличия вредоносного программного обеспечения в поступающих незапрашиваемых электронных сообщениях (письмах, документах).
4. Установите и обязательно обновляйте антивирусные программы на всех используемых устройствах – и себе, и родственникам.
5. Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках. Официальные адреса кредитных организаций указаны в перечне web-адресов кредитных организаций, размещенном на официальном сайте Банка России.
6. Никому не сообщайте персональные данные, а уж тем более пароли и коды.
7. Не храните данные карт на компьютере или в смартфоне.
8. Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.
9. Если вам поступает звонок якобы от службы безопасности банка, в котором вы обслуживаетесь, с информацией о том, что кто-то пытается с использованием ваших персональных данных взять кредит или осуществить несанкционированную операцию с вашего счета, не спешите следовать инструкциям злоумышленника. Положите трубку, перезвоните в банк по номеру телефона, указанному на банковской карте или на официальном сайте организации, и уточните полученную информацию.
10. Также вы можете изучить наши рекомендации по защите информации в разделе сайта «Информация для клиентов».