

Памятка о безопасности в сети Интернет

1. Не обращать внимания на звонки и смс, сообщения о выигрышах с незнакомых номеров, никогда не перезванивать на них, не отправлять сообщения;
2. Никому не сообщать реквизиты своей пластиковой карты, со всеми вопросами обращаться непосредственно в отделение банка;
3. Установить надежный антивирус на свои устройства и регулярно проводить полную проверку системы;
4. Покупать только лицензионное программное обеспечение;
5. Установить на своем компьютере антивирусную программу, следить за ее обновлением, реагировать на ее сообщения.
6. Существуют случаи рассылки вирусов, а также вскрытия крупнейших узлов бесплатной почты. Поэтому не исключено, что даже со знакомого адреса может прийти вирус. Если на вашу электронную почту пришло письмо с прикрепленным к нему незнакомым вложением, ни в коем случае нельзя открывать это вложение, а лучше сразу удалить и очистить корзину в программе чтения почты.
7. Никогда не посылать никому свой пароль.
8. При регистрации на сайте необходимо использовать для паролей трудно запоминаемый набор цифр, букв и знаков, причем включить в пароль не менее 6 символов. Об этом часто приходит подсказка при регистрации.
9. Не сохранять свои учетные данные (логин и пароль) для входа в систему на компьютере. После завершения работы с сайтом в Интернете обязательно пользуйтесь функцией завершения сеанса работы с браузером. Просто закрыть окно браузера или ввести другой адрес сайта недостаточно. Это касается и мобильных устройств. Многие программы (особенно программы для обмена мгновенными сообщениями) имеют функцию автоматического входа в систему, сохраняющую имя пользователя и пароль. Отключите эту функцию, чтобы никто, кроме вас, не смог войти в систему.
10. Не оставлять без присмотра компьютер с важными сведениями на экране. Закончив работу на общедоступном компьютере, воспользуйтесь функцией выхода из системы во всех программах и закройте все окна, в которых могут отображаться конфиденциальные данные.
11. Опасайтесь подглядывания через плечо. Работая на общедоступном компьютере или работая с банкоматом, следите за мошенниками, которые подглядывают через плечо, как вы вводите секретные пароли, чтобы потом получить доступ к вашим данным.
12. Убедитесь в достоверности информации, полученной по телефону от неизвестных, представившихся сотрудниками правоохранительных органов, радиостанции, оператора сотовой связи, чиновниками, вашими родственниками, знакомыми или прочими лицами.
13. Не торопитесь предпринимать действия по инструкциям неизвестных людей, полученным посредством телефонного звонка или SMS, в особенности, если их инструкции требуют перевода или передачи вами денежных средств каким-либо способом. Позвоните в Центр поддержки клиентов своего оператора и уточните информацию. Поспешные действия могут привести к финансовому ущербу.

14. Уточняйте у оператора стоимость платных номеров, предлагающих участие в акциях и викторинах, проводимых контент-провайдерами.
15. Не торопитесь давать телефон на «один звонок» незнакомому человеку. Помните, что в последнее время участились случаи краж телефонов именно таким способом.
16. Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей, а если есть сомнения – то и от известных. По возможности, установите на мобильное устройство одну из многих антивирусных программ.
17. Не спешите звонить или отправлять SMS на короткий номер, который обещает разблокировку компьютера от вируса или рекламирует сервис, основанный на доступе к персональным данным других людей. Уточните информацию у своего оператора.
18. Для разблокировки компьютера от вирусов используйте антивирусные программы известных разработчиков, в том числе бесплатные версии, размещенные на их сайтах. Не стоит верить сообщениям, гарантирующим избавление от вируса или исчезновение Интернет-баннера при отправке SMS на короткий номер.
19. Вы можете подключить услугу «Черно-белые списки», которая позволяет блокировать доступ к сервисам, предоставляемым контент-провайдерами по Вашему желанию.
20. Вам позвонили или прислали SMS с неизвестного номера с просьбой о помощи близкому человеку:
 1. Не впадайте в панику, не торопитесь переводить деньги.
 2. перезвоните родным и узнайте, все ли у них в порядке.
 3. Уточните, где находятся близкие, подключите услугу «Маячок».
21. Ваш аккаунт в социальной сети заблокирован. Для разблокировки Вас просят отправить SMS на «короткий» номер:
 1. Не торопитесь следовать инструкциям.
 2. Обратитесь к администрации социальной сети и мобильному оператору.
 3. Не доверяйте сомнительным источникам.
 4. Не размещайте в социальных сетях конфиденциальную информацию.
22. Вам прислали MMS-открытку с неизвестного номера:
 1. Не открывайте вложенный файл и не переходите по ссылкам.
 2. Удалите сообщение со ссылкой.
 3. Защитите свой телефон, подключив бесплатную услугу «Стоп-контент».
 4. Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков.