5 популярных схем,

которые используют мошенники в сети

1. «ПЕРЕВЕДИ МНЕ ДЕНЕГ, ПОЖАЛУЙСТА»

Как работает

Злоумышленники взламывают аккаунт пользователя в социальных сетях и рассылают такие просьбы от его имени. Если вы переведете деньги, то их получит не ваш знакомый из списка друзей, а мошенник.

Как защититься

Если получили такое сообщение, найдите способ проверить, действительно ли это ваш друг. Позвоните ему или задайте какой-нибудь вопрос, ответ на который мошенник точно не знает. А от взлома аккаунтов защитит надежный пароль и специальные [**технологии**](https://dnevnik.ru/ad/promo/kaspersky-a3) для его создания и хранения.

2. «ПРОЙДИТЕ ОПРОС И ПОЛУЧИТЕ  
10 000 РУБЛЕЙ!»

Как работает

Пользователю обещают легкий заработок — солидную сумму за прохождение опроса в интернете. У тех, кто пройдет такой опрос в надежде на денежный приз, мошенники сначала выведают личную информацию, а затем предложат внести «комиссию» или «сервисный сбор». Увы, после этого человек все равно ничего не получит, а вот деньги и личные данные попадут в руки мошенников.

Как защититься

Не участвуйте в сомнительных акциях из интернета. Бесплатный сыр бывает только в мышеловке. Используйте защитные решения, которые проверяют и блокируют фишинговые ссылки с подобными фейковыми акциями в сети.

3. «УВЕДОМЛЕНИЕ: ВАМ ДОСТУПНО ДЕНЕЖНОЕ ВОЗНАГРАЖДЕНИЕ!»

Как работает

Злоумышленники понимают, что многие пользователи уже привыкли к спам-сообщениям в почте и мессенджерах и зачастую просто игнорируют и удаляют их. А вот в **[Google Календаре](https://www.kaspersky.ru/blog/spam-through-google-services/22834/?campaign=kl-ru_dnevnikkts19_spp_ona_afm__onl_b2c_dnevnikru_lnk_______&utm_source=dnevnikru&utm_medium=special&utm_campaign=dnevnik_ru_kts_text" \t "_blank)** или, например, на **[YouTube](https://www.kaspersky.ru/blog/youtube-scam-videos/23256/?campaign=kl-ru_dnevnikkts19_spp_ona_afm__onl_b2c_dnevnikru_lnk_______&utm_source=dnevnikru&utm_medium=special&utm_campaign=dnevnik_ru_kts_text" \t "_blank)** всё не так очевидно. Тут вероятность, что мошенническое сообщение будет открыто, может быть немного выше.

Как защититься

Чтобы не стать жертвой мошенничества в Google Календарях, можно, например, отключить функцию автоматического уведомления в настройках календаря. А чтобы защитить себя и своих близких от фишинга в интернет-сервисах, лучше установить на свои устройства надежное защитное решение **[Kaspersky Total Security.](https://www.kaspersky.ru/total-security?campaign=kl-ru_dnevnikkts19_spp_ona_afm__onl_b2c_dnevnikru_lnk_______&utm_source=dnevnikru&utm_medium=special&utm_campaign=dnevnik_ru_kts_text" \t "_blank)**

4. «УВАЖАЕМАЯ ТАТЬЯНА СЕРГЕЕВНА! ВАШ БАНКОВСКИЙ СЧЕТ ЗАБЛОКИРОВАН В СВЯЗИ С ПОПЫТКОЙ ВЗЛОМА. ЧТОБЫ РАЗБЛОКИРОВАТЬ ЕГО, ПЕРЕЙДИТЕ ПО ССЫЛКЕ»

Как работает

Мошенники присылают вам такое письмо в надежде, что вы, поддавшись панике, не обратите внимание, что оно отправлено с «левого» адреса, пройдете по ссылке и введете данные банковской карты. Вам даже могут позвонить по телефону и, представившись сотрудниками банка, попросить продиктовать данные карты или логин и пароль от личного кабинета, чтобы решить вопрос с «подозрительными» трансакциями.

Как защититься

Будьте бдительны. Получая такие письма и сообщения, проверьте, действительно ли их прислал банк. Для этого достаточно просто позвонить или написать в службу поддержки. И помните: ни при каких условиях сотрудники банка не будут просить вас сообщить им конфиденциальную платежную информацию.

5. «ГДЕ ТЫ ЖИВЕШЬ? А КЕМ РАБОТАЮТ ТВОИ РОДИТЕЛИ?»

Как работает

[**По данным опроса,**](https://kids.kaspersky.ru/wp-content/uploads/sites/2/2019/04/190402_Children_Russia_Report_Practics-1.pdf?campaign=kl-ru_dnevnikkts19_spp_ona_afm__onl_b2c_dnevnikru_lnk_______&utm_source=dnevnikru&utm_medium=special&utm_campaign=dnevnik_ru_kts_text) который провела «Лаборатория Касперского», к 11% детей в возрасте 11-14 лет за последний год пытались втереться в доверие незнакомые взрослые. Мошенники преследуют разные цели: кто-то пытается узнать у детей информацию об их родителях, финансовом состоянии семьи, а кто-то под разными предлогами или угрозами просит прислать фотографии приватного содержания или назначить ребенку личную встречу.

Как защититься

Родителям стоит рассказывать детям о том, с какими угрозами они могут столкнуться в сети и как избежать неприятных ситуаций. Когда ребенок только начинает познавать мир социальных сетей, лучше воспользоваться специальными технологиями для детской онлайн-безопасности. Так, решение **[Kaspersky Safe Kids](https://www.kaspersky.ru/safe-kids?campaign=kl-ru_dnevnikkts19_spp_ona_afm__onl_b2c_dnevnikru_lnk_______&utm_source=dnevnikru&utm_medium=special&utm_campaign=dnevnik_ru_kts_text" \t "_blank)** уведомит родителя, если к ребенку добавится в друзья подозрительный пользователь, например, со значительной разницей в возрасте.