

*По материалам НЦПТИ (Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет)*

## **10 ВЕЩЕЙ, КОТОРЫЕ НЕЛЬЗЯ ПУБЛИКОВАТЬ В СОЦСЕТЯХ**

Известная шутка о том, что соцсети создали спецслужбы - не более, чем шутка. Однако, в любом случае есть информация исключительно для личного пользования, которую не следует сообщать посторонним.

Осторожность в «виртуальном мире» не менее важна, чем в реальном. Люди привыкли позволять в Сети то, что нельзя в обычной жизни. Например, ругаться на форумах не считаясь с нормами политкорректности и приличия и не боясь при этом «получить в морду». Однако вседозволенность часто приводит к потере осторожности.

Пользователи постоянно выкладывают в открытом доступе информацию о себе, совершенно не задумываясь о последствиях. Вконтакте, Одноклассники, Facebook или Twitter могут быть удобным способом для общения с друзьями и обмена информацией, но в некоторых случаях соцсети могут представлять большую опасность, прежде всего — для личных финансов. Кроме того, существуют вещи, которые могут испортить карьеру пользователя или репутацию фирмы в случае размещения их в аккаунтах. Так что для социальных сетей актуальна пословица «Молчание — золото».

### **1. Пароли и ключи к ним**

Во-первых, ни в коем случае нельзя хранить на своих страницах или сообщать пароли от соцсетей, почтовых ящиков. Вроде бы, все логично. Однако, оказывается, многие интернет-пользователи пренебрегают даже такими очевидными мерами безопасности. Они легко сообщают пароли в общении даже с незнакомыми им сетевыми пользователями, а затем сталкиваются с тем, что их страницы были взломаны.

Кроме того, при регистрации в различных сервисах зачастую приходится отвечать на десяток вопросов для «защиты». Многие банки или онлайнмагазины знают девичью фамилию вашей матери, кличку домашнего животного, название любимой песни или футбольной команды. Если же все эти данные хранятся в ваших профилях — это значительно облегчает работу жуликам, являясь ключом к подбору ваших паролей. По той же причине не рекомендуется афишировать в соцсетях номера учебных заведений.

### **2. Дата и место рождения**

Указывать дату рождения предпочитают большинство пользователей, однако сообщая число, год и место своего рождения вы невольно помогаете аферистам похитить вашу финансовую информацию. Благодаря этим данным злоумышленники смогут попытаться узнать номера вашего паспорта,

страхового и пенсионного свидетельства, и других документов. В дальнейшем они могут использовать эту информацию в мошеннических целях.

### **3. Номер телефона**

Различные мошенники с радостью воспользуются предоставленным в соцсетях номером телефона, не скрытым настройками приватности. Помимо того, что у многих пользователей банковские карты привязаны к телефонным номерам, рекламодатели также с удовольствием воспользуются вашим номером. На оставленный в открытом доступе номер телефона может сыпаться «спам» или, например, сообщения от мошенников с требованием оплаты несуществующих кредитов.

### **4. Домашний адрес и имущество**

Любое упоминание или намек на ваш домашний адрес ставит вас под угрозу. Злоумышленники могут использовать эту информацию, особенно если знают, в какие часы вас не бывает дома. Если вы не хотите стать жертвой грабежа, мошенничества и хакерских атак, то не указывайте свой домашний адрес. Кроме того, не следует размещать фотографии и описание каких-либо достопримечательностей, расположенных по соседству. Даже вид из окна может привлечь преступников. Тем более, нельзя публиковать фотографии с ценными вещами, которые находятся в квартире.

### **5. Платежные реквизиты**

Не стоит оставлять в соцсетях свою платежную информацию или оплачивать в них дополнительные услуги банковскими картами. Оплата непосредственно через сайты тех же онлайн игр небезопасна. Это вам подтвердят в любом банке, карта которого у вас на руках. В случае, если аккаунт будет взломан, и злоумышленники «утянут» все деньги со счета, то доказать тем же банкам, то это не вы потратили все ваши сбережения, будет очень сложно. Нельзя также сообщать о размере вашей заработной платы или о том, где вы ее получаете и храните.

### **6. Данные о работе**

Не следует оставлять на вашей страничке в соцсетях любую информацию, связанную с вашей работой. Из-за болтливости сотрудников журналистам неоднократно удавалось получить данные о каких-либо новинках или планах компании за несколько месяцев до их официального обнародования. Кроме того, необходимо помнить, что на вашу страницу могут зайти начальник или коллеги и увидеть сообщения или фотографии, которые им не понравятся. Работодатели довольно часто просматривают социальные сети в поисках возможных сотрудников. Они могут прочитать записи о прошлом месте работы и сделать выводы о вас. Не позволяйте себе писать сообщения, в которых вы жалуетесь на свою работу, начальника или коллег. Даже один негативный твит может испортить вам репутацию. Не стоит и размещать фотографии с вечеринок и корпоративов. Обсуждать свои планы на вечер и выходные в рабочее время также не следует. Кроме того, помните, что говорите на работе. Известно немало случаев, когда человек, отпросившись с работы по причине плохого самочувствия, выкладывал фотографии с какой-нибудь вечеринки или пляжа, а работодатель наблюдал затем в Сети, как «страдает» их «тяжелобольной сотрудник». Вообще, стоит удалить из соцсетей

любые сомнительные фотографии. Вряд ли работодателям понравится ваше фото в пьяном виде, даже если фотографии лет 10.

### **7. Планы на отпуск или выходные**

Нельзя сообщать сроки и место проведения планируемого отпуска. Такие сообщения, как «Ура, завтра я на 2 недели еду на море!» — превращают вашу квартиру в цель для взломщиков. По той же причине не следует писать сообщения или ставить «отпускные» статусы, находясь на каком-нибудь пляже. Если пожелаете, вы можете выложить фото, когда вернетесь, но не стоит сообщать возможным вора́м о вашем отсутствии. Ограбление в этом случае может произойти, даже если вы не оставляли на сайте свой реальный адрес.

### **8. Данные об отношениях**

Встречаетесь вы с кем-нибудь, находитесь в браке или в ваших отношениях «все сложно» — не стоит выставлять эту личную информацию на ресурсах общего пользования. Статус, рассказывающий в ваших соцсетях об отношениях, может также притягивать киберпреступников. Существует немало примеров, как доверчивые пользователи попадались в сети мошенников, «разводивших» их на откровенные разговоры, фотографии и другую информацию, которая в дальнейшем использовалась для шантажа.

### **9. Экстремальные хобби и вредные привычки**

Если увлекаетесь экстремальными видами спорта и часто подвергаете свою жизнь опасности, то об этом сообщать не нужно. Большинство ругеров, бейс-джамперов и других экстремалов предпочитают создавать фейковые аккаунты, и это правильно. В эпоху, когда Интернет превратился в глобальную базу данных, подобная информация может скомпрометировать вас в глазах страховой фирмы. Помимо страховых компаний все больше используют Интернет для составления «портрета» клиента и банки. Пока отмена страховок, отказ в выдаче кредитов или повышение процентных ставок на основании повышенных рисков для жизни заемщика в России еще не применялись. Однако в Европе известны подобные случаи из-за «несоответствия» страницы в социальной сети и описания в заявлении заемщика. Об этом следует помнить не только любителям экстрима, но и любителям «смолить как паровоз».

### **10. Публичные сообщения на вашей «стене»**

Сообщения ваших друзей, знакомых или вовсе неизвестных людей, опубликованные на вашей «стене» также могут сыграть негативную роль в реальной жизни. Шутки «ниже пояса», «оскорбления», «обвинения», которые позволительны при непосредственном общении, не должны становиться достоянием общественности. Нельзя забывать, что подобные «шедевры» видит не только получатель, но и другие пользователи, не посвященные в тонкости вашего общения. Перед тем, как отправить очередное сообщение провокационного содержания, задумайтесь, не навредит ли оно адресату. Кроме того, собственную «стену» надо регулярно проверять и, в случае появления, обязательно удалять подобные сообщения. Желательно ограничить список пользователей, которым разрешена публикация сообщений на «стене». Помимо постов от друзей, «стену» могут засорять сообщения из сообществ, в которых вы состоите, и другой спам.