**Утрата денег**

Первый вид опасностей – те, которые связаны с кражей денег.

**Фишинг** – это выманивание паролей от различных сервисов, в том числе личных страниц во «ВКонтакте» или Steam, чем дети-подростки обычно очень дорожат. Их крадут, чтобы получить доступ к персональной информации, чтобы делать спам-рассылки, чтобы продолжать использовать – например, аккаунты игровой платформы Steam, где распространяются игры и есть своя социальная сеть.

Steam – это рекордсмен по числу онлайн-пользователей, их там больше, чем даже в YouTube. Поскольку участники покупают игры на свой аккаунт, «развивают» своих персонажей в многопользовательских онлайн-играх, «заливают» туда деньги и время, эти аккаунты могут достаточно дорого стоить – страничка с 1000 наигранных часов в какую-нибудь популярную многопользовательскую игру с очень развитым персонажем продастся на черном рынке за весьма неплохие деньги.

Еще одна техническая опасность – **вредоносный код**: например, пользователь перешел по какой-то ссылке, и компьютер заблокировался, и теперь пользователь видит только сообщение «Заплатите деньги туда-то, и компьютер разблокируется». Причем гарантии, что он разблокируется после оплаты, к сожалению, нет. Есть и другой вредоносный код: тот, что незаметно работает на компьютере, отправляя злоумышленникам те же логины/пароли или данные платежных карт.

**Обычное мошенничество** – в интернете встречается так же часто, как и в реальной жизни. Его можно охарактеризовать всем известной поговоркой «Бесплатный сыр бывает только в мышеловке». Например, предлагается купить смартфон по цене значительно ниже рыночной, человек отправляет деньги, но телефон так и не получает. Это очень популярная схема мошенничества: дорогой товар за небольшие деньги. И это очень хорошо срабатывает в ситуации с подростками, потому что они часто прицельно копят деньги на какой-нибудь игровой компьютер, и если они внезапно видят его не за 60, а за 20 тысяч рублей, то могут с радостью заказать его и перевести деньги.

Определенную опасность для семейного бюджета представляют также и онлайн-игры – в них часто есть **встроенные внутренние покупки**. Чтобы обезопасить себя от этих трат, убедитесь, что ребенок не может тратить деньги с вашей карточки, привязанной к онлайн-игре, в том числе и если он зайдет в вашу игру.

Это может происходить, если система запрашивает подтверждение не каждый раз при совершении покупки, а, например, раз в полчаса, раз в сутки. За полчаса можно многое успеть. Одна английская девочка четырех лет, играя, пока папа варил макароны, потратила больше 1000 фунтов, причем ругать ее было за это бесполезно: она просто играла и даже не знала, что тратит деньги, нажимая на «да» и «купить».