Интервью с хакером: как спасти персональные данные?

04.06.2025

Практически каждому из нас сложно представить свою жизнь без интернета и мобильных устройств. Тем не менее, пользователи помнят, что мошенники с появлением современных технологий тоже адаптировались. Россияне, в число которых входят и сибиряки, всё чаще подвергаются кибератакам преступников, орудующих в сети Интернет.

Согласно статистике Red Secutiy, за первый квартал 2025 года Сибирь подвергалась DDoS-атакам чаще, чем другие округа России. Напомним, что недавно произошла атака на интернет-провайдера «Сибсети». Злоумышленники массово направляли на сайты запросы, из-за чего система была перегружена и вышла из строя.

Кроме DDoS-атак мошенники находят и другие, более простые с технической точки зрения, способы навредить пользователям. Например, недавно аферисты выдавали себя за мэра Бердска Семена Лапицкого. Они создали внешне похожий аккаунт в мессенджере и писали местным жителям в личные сообщения, что их диалог должен остаться в секрете.
Так, жители Новосибирской области периодически сталкиваются с нападками как хакеров-злоумышленников, так и обычных мошенников, работающих через соцсети.

Сейчас существует много мошеннических схем, которые используют на просторах сети. Тем не менее, если от некоторых их видов обычные пользователи могут себя оградить при помощи бдительности, то от других – нет. Человеку, который не связан с IT-сферой, многое кажется непонятным. Редакция НДН.инфо связалась с российским хакером, программистом и автором книг по безопасности в Сети,

Дмитрием Артимовичем, чтобы разобраться, где опасность мнимая, а где реальная. Уточним, что широкую известность он получил после организации DDoS-атаки на серверы процессинговой компании Assist, из-за которой с 15 по 24 июля 2010 года клиенты «Аэрофлота» не могли совершать покупки на сайте авиакомпании.

Фото: Дмитрий Артимович

В интервью эксперт рассказал, безопасен ли VPN, как мошенники могут залезть в личные переписки пользователей и почему новосибирцам не стоит бояться киберперступных группировок.

VPN — есть ли угроза утечки данных?

Сейчас в России ограничен доступ к ряду социальных сетей и мессенджеров, из-за чего пользователи стали активнее пользоваться VPN — Virtual Private Network. Это частная сеть, которая шифрует интернет-трафик, присваивая IP-адрес другой страны, благодаря чему россияне могут пользоваться заблокированными сайтами. Тем не менее, жителей страны предупреждают об опасности использования частной сети. Ею же обосновывают блокировку приложений VPN.

По словам Дмитрия Артимовича, угроза шифрования интернет-трафика — миф. Более того, он считает, что VPN, наоборот, помогает сохранить приватность. Блокировку сервисов для шифрования трафика он относит к политике и отрицает

её причастность к заботе о кибербезопасности россиян.

> «Не очень понимаю, про какие риски вы говорите. Я, например, использую VPN, чтобы мой трафик не смотрели», — прокомментировал он.

Кто читает наши переписки?

Один из самых распространённых страхов пользователей — проникновение злоумышленников в их личные переписки. Не секрет, что иногда в наших диалогах хранится информация, которая может стать поводом для шантажа или позволит мошенникам «вытянуть» деньги. Например, пароли, данные банковской карты, адрес проживания и прочее.

По словам Дмитрия Артимовича, вероятность, что такое произойдёт без ведома пользователя, крайне мала.

> «С современных телефонов сложно что-то украсть. Только, если обманом заставить человека сделать это своими руками. Например, перевести деньги на якобы „безопасный счет“. Однако этим занимаются не хакеры, а мошенники», — объяснил эксперт.

Также Дмитрий Артимович подчеркнул, что некоторые наши действия могут оказаться необратимыми, поэтому от осторожности и осведомленности напрямую зависит, попадётся ли пользователь «на крючок» злоумышленника.

> «Если сам передал доступы, прочитал СМС третьим лицам — с большой вероятностью, уже ничего не вернёшь. Нужно обучать население финансовой грамотности», — подытожил эксперт.

Преступление по-крупному: опасны ли киберперступные группировки для новосибирцев?

Сейчас самой опасной и загадочной киберперступной организацией считают Qilin. Преступники из этой группировки, также известной под названием Agenda, занимаются кражей или шифровкой данных, из-за которой невозможно получить к ним доступ, после чего требуют выкуп. Так, злоумышленники атакуют зарубежные больницы и суды уже около трёх лет. Например, в прошлом году они помешали работе нескольких лондонских медицинских учреждений. Также Qilin атаковали американскую организацию Promises2Kids, которая занимается помощью детям.

По предположениям специалистов, эти мошенники являются русскоязычными хакерами. Группировка Qilin часто использует фишинг, чтобы найти новых жертв для кражи данных. Так, преступники выманивают информацию пользователей разными путями. Известно, что киберпреступники также имеют свой сайт в

даркнете, куда «утекает» ворованная информация.

Мы спросили Дмитрия Артимовича, представляют ли угрозу для обычных пользователей такие «акулы» киберпреступного сообщества, как, например, группировка Qilin (Agenda).

> «Их интересуют те, у кого есть данные, и кто сможет заплатить выкуп. С обычного пользователя мало можно взять», — объяснил эксперт.

Тем не менее, вредоносные вирусы может «подцепить» любой интернет-пользователь. По словам Дмитрия Артимовича, обычно такая угроза поджидает на сайтах «для взрослых» и сайтах с «ломаным программным обеспечением», то есть таким, которое было нелегально скопировано. Также у «ломаного ПО» обычно взломаны защиты и пароли для входа.

Напомним, что с начала текущего года жертвами мошенников на просторах сети всё чаще становятся дети и подростки.

Александра Моисеева