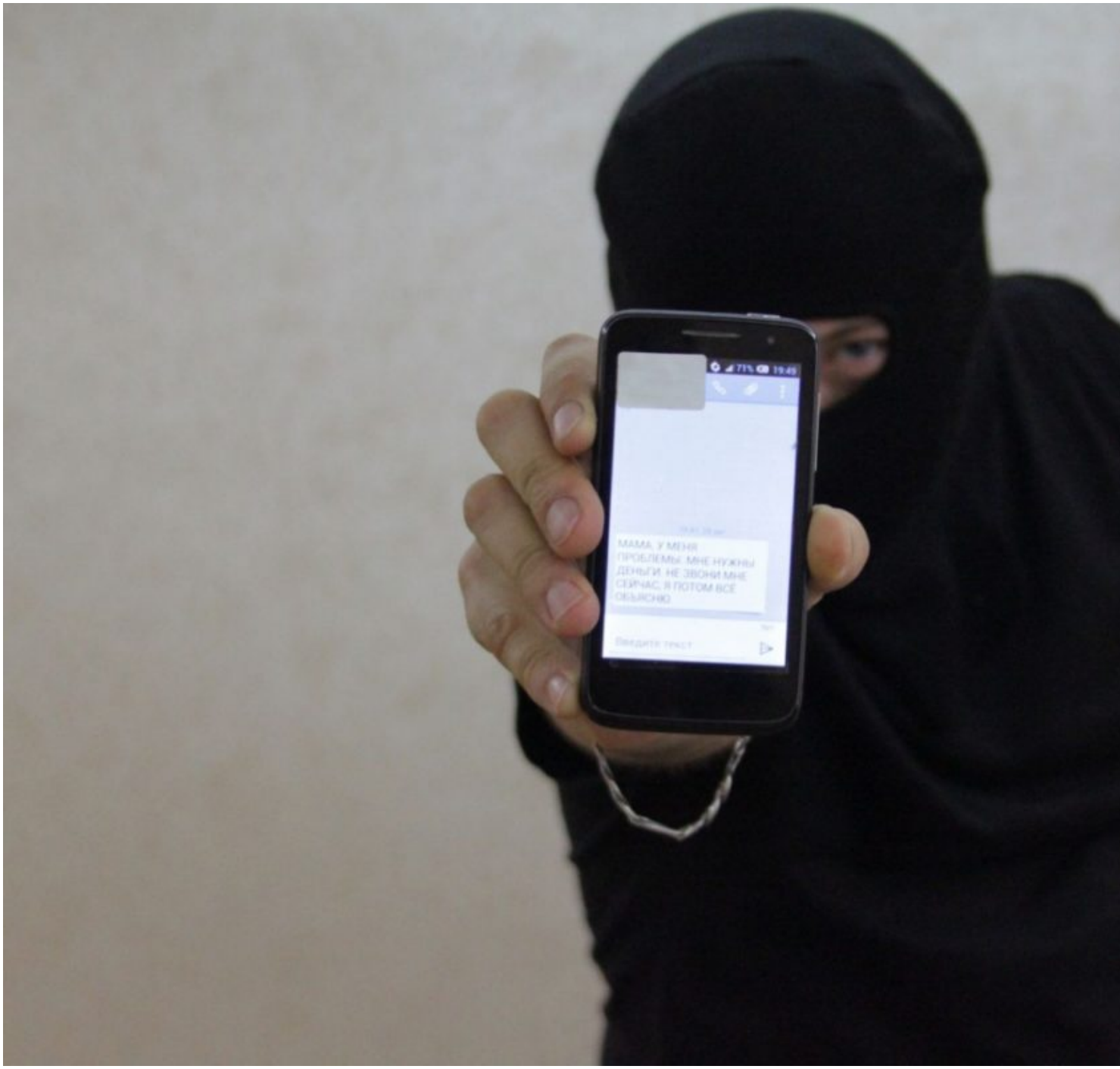
Не дайте обмануть себя: защитите свой телефон от мошенников

Автор: Administrator
20.07.2019 17:51 -

Мошенники постоянно придумывают новые ухищренные способы обмана добропорядочных пользователей. Чтобы защитить свой гаджет и свои сбережения от киберворов, нужно всего лишь следовать простым рекомендациям.



Установите приложение интернет-безопасности

Зачастую вредоносные программы попадают в наши смартфоны после установки очередного приложения, скачанного с непроверенного сайта. После этого вирус как спрут проникает своими щупальцами в операционную систему и заражает файлы. Мошенники создают вирусы, маскирующиеся под безобидные файлы и приложения, которые пользователь без раздумий и сомнений скачивает под видом полезного контента. Это могут быть различные виды файлов: книги, документы, картинки, фильмы и видеоролики, музыка и многое другое. После установки вредоносного ПО вирус начинает воровать информацию, отправлять пароли, рассылать сообщения от вашего имени, вмешиваться в нормальную работу устройства и даже блокировать телефон.

Чтобы избежать такого поворота событий, нужно соблюдать следующие правила:

- установить антивирусную программу и периодически проверять смартфон на наличие вирусов
- загружать обновления операционной системы и скачивать приложения только от разработчиков
- использовать лицензионные программы и доверять только проверенным источникам
- не открывать ссылки, полученные по электронной почте, в SMS и MMS от незнакомых пользователей, удалять подозрительные сообщения еще до прочтения
- не сообщать никому пароли, учетные записи и прочую личную информацию.

С программой для интернет-безопасности ваш гаджет будет под всегда под надежной защитой, такие софты выявляют и блокируют работу вредоносных приложений. Регулярное обновление этих программ происходит автоматически при подключении к сети.

Проверяйте ссылки, на который переходите

URL — это путь к интернет-ресурсу, по которому можно найти интересующую вас информацию. В настоящее время URL является идентификатором адресов всех ресурсов, размещенных в сети. Это адрес страницы, на которой мы находимся, размещается он в адресной строке вашего браузера и, как правило, находится в самом вверху.

Классический пример URL-адреса: http://адрес_сайта/папка/страница.html

Перед адресом обычно отображаются латинские буквы https. Это протокол с поддержкой шифрования, который обеспечивает безопасное соединение и обмен данными между сайтом и пользователем. Иначе говоря, обозначение «https:» гарантирует безопасность сайта.

Проверка URL-адреса перед посещением сайта является основой безопасности мобильного интернета. Внимательно вчитывайтесь в написание доменов, злоумышленники маскируют их под известные сайты, изменяя или добавляя одну букву, поэтому при беглом взгляде разглядеть подвох практически невозможно.

При переходе на сайт тщательно проверяйте URL-адрес, особенно этим нельзя пренебрегать при переводе денежных средств и вводе важной информации.

Планируя дорогую покупку не поленитесь проверить информацию о продавце и интернет-магазине. Наведите справки, почитайте отзывы реальных покупателей.

Исследуйте приложение перед скачиванием

Не загружайте мобильные приложения на свой гаджет, предварительно не проверив его происхождение. Найдите отзывы пользователей об этой программе, почитайте рейтинги, рекомендации — под безобидной программой может скрываться сайт мошенников. При открытии ссылки программа автоматически запускает отправку сообщений на платные номера, рассылает личные файлы без вашего ведома, тем самым ставя под удар безопасность мобильного гаджета и ваши конфиденциальные данные.

Мобильные жулики идут в ногу со временем и стараются не отставать от технического прогресса. Они придумывают новые способы завладеть вашими деньгами и уделяют большое значение разработке новых софтов и программного обеспечения. У многих есть знакомые, которые хоть раз скачивали программу или открывали неизвестную ссылку, и в итоге с мобильного счёта списывались деньги.

Чтобы не попасться на уловки злоумышленников, нужно скачивать информацию на телефон или компьютер из проверенных источников, которым вы доверяете. Например, для каждой операционной системы для смартфонов и прочих гаджетов разработчики предлагают целый магазин приложений, в котором можно без труда найти интересующую программу.

Не рассказывайте личную информацию о себе незнакомым лицам: логин и пароль от личного кабинета, кодовые слова, одноразовые пароли должны держаться в тайне. Если по телефону сотрудник банка или другой организации просит предоставить конфиденциальные данные — знайте, что это мошенники, и они хотят воспользоваться вашей доверчивостью. Запомните также, что работники банка никогда не просят продиктовать личные данные по телефону.

Для защиты своего телефона от мобильных мошенников используйте все возможные средства и будьте бдительны. Такая осторожность поможет сохранить денежные средства на счете телефона в целости и сохранности и избежать многих неприятностей.

(**Голосов: 1**; Рейтинг: **4,00** из 5)

Загрузка...