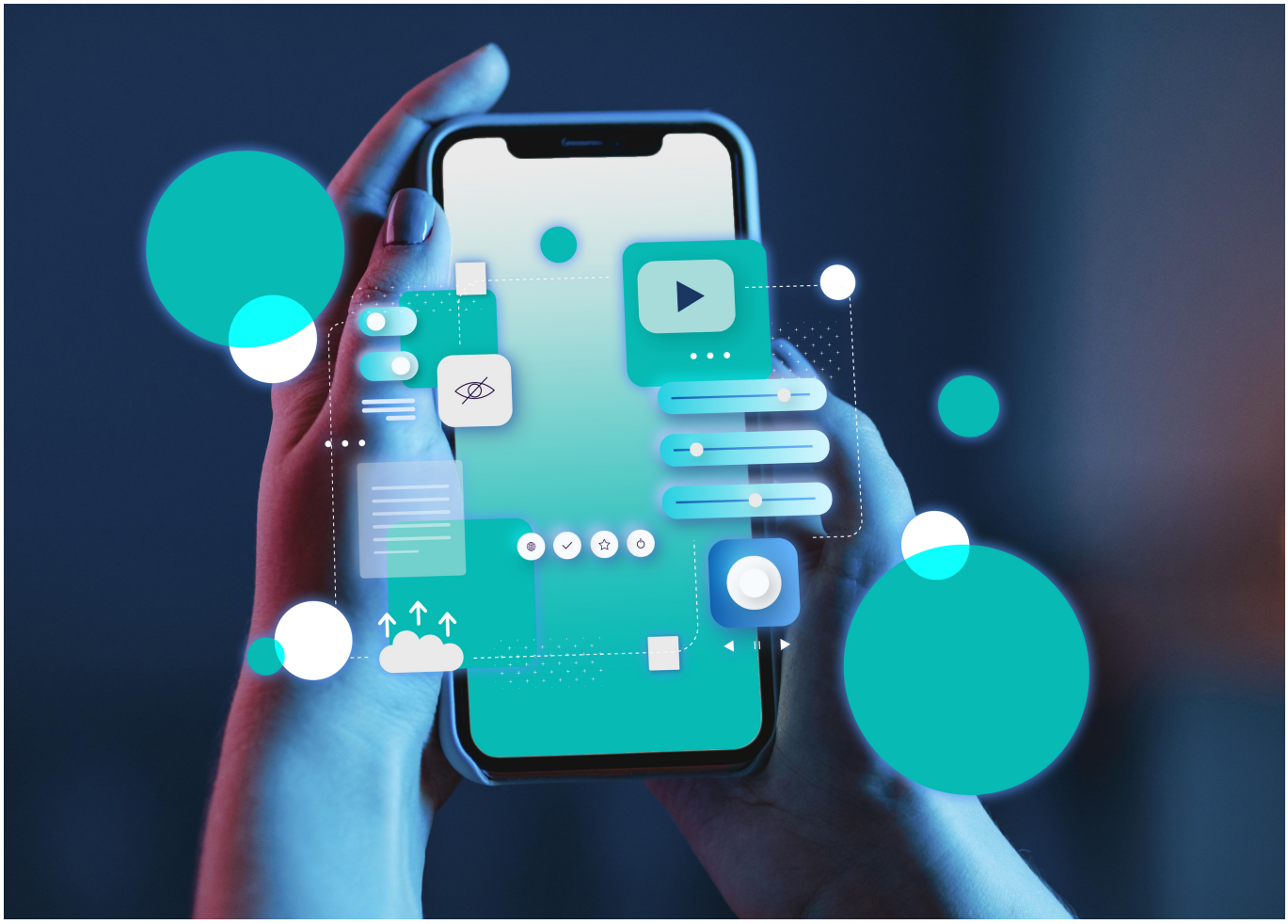
Многие из нас даже не задумываются, что предоставление некоторых разрешений мобильным приложениям может быть рискованным. Вот какие разрешения самые опасные.

Доступ к контактам. Злоумышленники могут этим пользоваться, чтобы получить доступ к данным человека, рассылать спам, осуществлять фишинг. Предоставляйте такое разрешение лишь проверенным приложениям, а также регулярно проверяйте, у каких приложений есть доступ к вашим контактам.

Камера и микрофон. Некоторые приложения могут за счёт этого вести скрытую запись действий пользователя, прослушивать, что вокруг вас происходит. Включайте микрофон и камеру только тогда, когда они вам действительно нужны. После завершения работы отключайте доступ к ним для приложений.

Местоположение. Разрешайте доступ к нему только надёжным приложениям.



freepik

Звонки и СМС. Мошенники используют доступ к ним для массовой рассылки рекламных предложений или платных подписок. Избегайте установки приложений, которые запрашивают это разрешение, хотя оно не связано с основной работой программы.

Файлы и хранилище. Некоторые вредоносные программы могут за счёт доступа к файлам и хранилищу заразить устройство вирусами или похитить данные. Поэтому устанавливайте только проверенные приложения.

Контроль над уведомлениями. Лучше отключать его для всех приложений, кроме тех, которые вам нужны ежедневно.