Пресс-релиз

«Тихий захват WhatsApp» без взлома и следов.

Центр прогнозирования преступных угроз и рисков общественной безопасности Комитета по правовой статистике и специальным учетам Генеральной прокуратуры предупреждает о новой киберугрозе, связанной с мессенджером «WhatsApp».

По данным зарубежных источников (https://infobezopasnost.ru/blog/news/kiberataka-ghostpairing-pozvolyaet-moshennikam-poluchit-polnyj-dostup-k-whatsapp-bez-vzloma-parolya/, https://www.securitylab.ru/news/567291.php, https://securitymedia.org/news/list/ataka-ghostpairing-pozvolyaet-nezametno-zakhvatyvat-akkaunty-whatsapp.html) кибермошенники запустили новую криминальную схему захвата аккаунтов «WhatsApp». Этот метод получил название «GhostPairing», он не требует взлома паролей, подмены SIM-карт или сложных технических атак, в Ваш «WhatsApp» проникают легально, активируя функцию по привязке дополнительных устройств.

Сценарий прост – отправляется сообщение, замаскированное под «Facebook», «WhatsApp», перенаправляющая пользователя на поддельные страницы, визуально копирующие интерфейс «Facebook, WhatsApp».

Для подтверждения доступа к контенту, фейковый сайт предлагает ввести номер телефона и код подтверждения, после чего злоумышленник автоматически добавляется в аккаунт жертвы как доверенное устройство, получая полный доступ к «WhatsApp» (чтение сообщений, просмотр медиафайлов, контактов, отправка сообщений, доступ к фотогалереи), при этом телефон продолжает работать как обычно, не вызывая подозрений.

Единственный способ обнаружить захват «WhatsApp» - вручную проверить раздел «Связанные устройства». Любое неизвестное подключение - указывает на компрометацию и подлежит немедленному удалению.

Будьте бдительными, соблюдайте кибербезопасность:

- критически относитесь к неизвестным входящим сообщениям, звонкам и различным уведомлениям;
- не вводите код «WhatsApp» на сторонних сайтах, запрос кода вне приложения – всегда мошенничество;
- используйте двухфакторную аутентификацию;
- регулярно проверяйте активность Вашего аккаунта;
- используйте защитные программные обеспечения.

Цена одной ошибки - полный контроль над Вашей личной перепиской.