• КЦ ИРНИТУ •

#профилактика

СКИММИНГ

Скимминг (от англ. to skin - бегло прочитывать, скользить) - копирование данных с магнитной полосы банковской карты.

Мошенники могут устанавливать переносные считыватели в гостиницах, кафе и ресторанах, в магазинах, чтобы заполучить нужные им данные.

• КЦ ИРНИТУ •

#профилактика

ФИШИНГ

Фишинг (от англ. phone phreaking - взлом телефонных автоматов и fishing - рыбная ловля) - интернет-мошенничество. Применяется для кражи паролей, номеров карт, банковских счетов и другой конфиденциальной информации.

Фишинговая атака представляет собой выдачу фейковых сайтов, имитирующих страницы популярных компаний, где пользователи могут ввести свои данные (но делать этого не нужно).

• КЦ ИРНИТУ •

#профилактика

ВИШИНГ

Вишинг (от англ. voice phishing, то есть голосовой фишинг) - разновидность фишинга с использованием голоса.

Цель вишинга, телефонного мошенничества, банальна - узнать данные жертвы: номер карты, код из SMS, данные паспорта, пароль от соцсети. Или с помощью методов социальной инжинерии уговорить человека перевести деньги на счет мошенника.

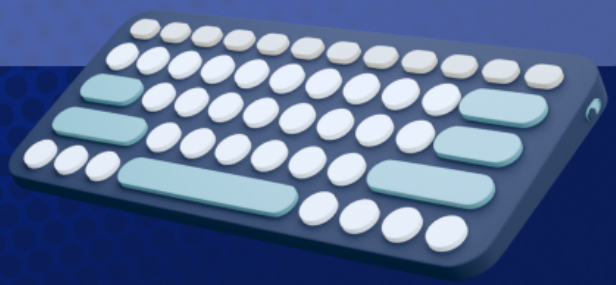
• КЦ ИРНИТУ •

#профилактика

ФАРМИНГ

Фарминг (от англ. pharming - производное от phishing и farming - занятие сельским хозяйством) - вид кибератаки, с целью скрытного перенаправления пользователя на фишинговый ресурс злоумышленника при помощи вредоносного ПО, установленного на компьютер жертвы.

Основновные цели фарминга - пользователи онлайн-банков или других финансовых систем и валютно-обменных сервисов.



• КЦ ИРНИТУ •

#профилактика

СНИФФЕРИНГ

Снифферинг (от англ. to sniff - вынюхивать) - способ мошенничества, при котором злоумышленник использует анализатор проходящего интернет-трафика - сниффер. Это специальная компьютерная программа для перехвата данных.

Снифферинг особенно популярен в людных местах - например, там, где есть общедоступная сеть Wi-Fi. С помощью этой схемы мошенники могут узнать, например, логины и пароли жертв.