УГРОЗЫ В ИНТЕРНЕТЕ

И СПОСОБЫ ОТ НИХ ЗАЩИТИТЬСЯ

Мы все в целом знаем, что значит безопасное поведение в интернете. Тем не менее каждый день мошенники получают доступ к личным данным пользователей, крадут деньги с их счетов, оформляют кредиты онлайн.

Мы хотим напомнить о главных опасностях в сети и способах от них защититься.

🔹 Вредоносные файлы и программы

Любые файлы или программы могут быть использованы для нанесения вреда пользователю. Вы можете случайно скачать вирус или программу-вымогатель, которая блокирует файлы и угрожает пользователю стереть данные или выложить их в общий доступ, если тот не переведёт определённую сумму.

Как защититься?

— Использовать антивирус.

— Не переходить по неизвестным ссылкам.

— Не скачивать непонятные файлы.

— Устанавливать приложения только из надёжных источников (официальные сайты и магазины приложений).

🔹 Социальная инженерия (фишинг)

Социальная инженерия — это атака, основанная на взаимодействии киберпреступника с пользователем. Например, жертвам рассылаются мошеннические электронные письма, похожие на сообщения из авторитетных или известных источников. Цель таких атак — украсть конфиденциальные данные.

Как защититься?

— Установить двухфакторную идентификацию везде, где это возможно.

— Внимательно проверять адрес почты, с которой пришло письмо со ссылками или вопросами. Если адрес неизвестен, не переходить по ссылкам и не открывать вложения.

— Проверять подлинность сайтов, на которых нужно ввести пароль (например, вместо vk.com мошенники могут использовать vc.com).

— Никому не сообщать пароли и коды для входа — их спрашивают только мошенники.

🔹 Атаки «человек посередине»

При такой атаке киберпреступник перехватывает и передаёт сообщения между двумя сторонами для кражи данных. Например, между гостевым устройством и сетью в незащищённой сети Wi-Fi.

Как защититься?

— В идеале не использовать неизвестные сети Wi-Fi (в кафе, на вокзалах и т.д.), а пользоваться мобильным интернетом.

— Если всё же использовать общественный Wi-Fi необходимо, не вносите через такую сеть платёжную информацию на сайты и не используйте банковские приложения, пользуйтесь только сайтами с цифровым сертификатом безопасности HTTPS.

И ещё несколько простых правил, которые все знают и почти все нарушают:

🔹 При создании пароля придумывайте сложные комбинации или используйте специальные генераторы.

🔹 Периодически меняйте пароль на новый.

🔹 Не используйте один и тот же пароль для нескольких сайтов.

🔹 Старайтесь не входить в свои личные кабинеты с других устройств. А если всё-таки зашли, не забывайте выходить из них.

🔹 Помните, что любой ваш собеседник в мессенджерах может быть взломан в любую минуту. Имейте это в виду, когда переводите деньги по его просьбе или высылаете личные файлы.

#советы_просвещение