**ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ**

**1. Не полагайтесь только на свой ум, доверяйте программам**

Человек — основная проблема кибербезопасности, причем любой: и корпоративной и личной. Об этом стоит всегда помнить. Если раньше хакеры были прежде всего технически подготовленными людьми, которые осуществляли атаки, пользуясь уязвимостями, то сегодня злоумышленники в сети — это в первую очередь умные психологи-профессионалы. Технические решения не сильно защитят от угроз, если по ту сторону экрана в составе преступной группировки работают профи. Они изучают поведение людей, описывают методы, которыми люди пользуются, а уже на основе этих данных совершают киберпреступления.

У киберпреступников много разных тактик. Самая распространенная — отправка сообщений по электронной почте, которые выглядят как настоящие, отправленные якобы с настоящего домена, например, «Сбербанка» или налоговой службы. Если пользователь торопится, он не увидит разницы: на глаз невозможно определить, чем отличается настоящее сообщение от фейкового. Киберпреступники, например, заменяют символы английского алфавита на русские, и в итоге адрес выглядит как настоящий.

Увы, классический совет — «не открывайте письма от незнакомых людей» — давно не работает. Обязательно надо использовать специальные настройки браузеров или почтовых клиентов, которые отслеживают и отсекают фальшивые сообщения.

**2. Не доверяйте незнакомым «друзьям», даже если они сильно похожи на вас**

Хакеры не теряют время: они тратят недели и месяцы на то, чтобы составить психологический портрет жертвы. Изучают ваши привычки, любимую музыку и фильмы, следят, где вы отдыхаете, и в итоге составляют ваш профиль. Они делают это не вручную, а используя искусственный интеллект. Технологии машинного обучения позволяют создать фотографию подходящего «друга», исходя из данных о вас: по вашим лайкам можно определить, какие люди вам нравятся внешне, а какие нет. В итоге хакеры, учитывая всю специфику, создают фейковый аккаунт пользователя, но такого, с которым вам точно захочется дружить — ведь он будет похож на человека из вашего круга общения. Когда вы добавите его в друзья, то вероятность того, что вы будете доверять его личным сообщениям, станет достаточно высокой.

Как отличить бота от реального человека? Проведите проверку: спросите пользователя об общих с вашими интересах. Если это не бот, а живой человек, то нужно сопоставить, насколько то, что у него написано в профиле, соответствует тому, что он реально пишет в ответах в чате.

**3. Не хотите бесплатно майнить чужую криптовалюту? Регулярно обновляйте софт**

Уж сколько раз твердили миру… обновляйте программы на компьютере регулярно или поставьте галочку на автоматическое обновление. Обновлять надо не только программы, но и плагины, например, к браузерам — минимум раз в неделю. Именно через них киберпреступники устанавливают контроль над пользователями и используют ваш компьютер для рассылки спама, вирусов, организуют DDoS-атаки.

Очень полезно установить дополнительные бесплатные расширения для браузера, которые заблокируют запуск вредоносных скриптов, если вы зашли на вредоносный сайт. Задача таких скриптов — установить контроль над компьютером пользователя или использовать его, например, для майнинга криптовалют. Такие расширения, как NoScript, uMatrix или JS Blocker, отключают ненужные скрипты на большинстве сайтов.

Стоит пользоваться и блокировщиками рекламы. Киберпреступники нередко арендуют рекламные площади и ставят туда баннеры с вредоносным кодом, который запускается, если пользователь кликает по нему. В итоге компьютер заражается, или пользователь попадает на вредоносный сайт. Нередко такие сайты выглядят как настоящие, но в действительности лишь имитируют интерфейс почтового клиента или интернет-банка. Доверчивый пользователь вводит логин и пароль, а хакеры получают доступ к его почтовому ящику или крадут данные о банковском аккаунте. В названии сайта может быть изменена всего одна буква, это часто трудно заметить. Кстати, вероятность попадания на такой сайт с планшета или смартфона выше, ведь в этом случае строка браузера небольшая, и отследить ошибку на маленьком экране труднее.

И да, это не миф: пользователи Android рискуют больше, чем пользователи Apple. Платформа Apple iOS более закрытая, поэтому не все разработчики имеют доступ к внутренностям системы. К тому же разместить приложение в Google Play гораздо проще, чем в Apple Store, поэтому число вредоносных программ там выше. Большинство банковских «троянов», которые крадут деньги со смартфонов, сделаны на Android, для продуктов Apple их почти не пишут.

**4. Не будьте самоуверенны**

Еще одна распространенная проблема пользователей — уверенность в том, что они хорошо и безошибочно печатают на клавиатуре. Проблема чаще возникает на смартфонах и на планшетах: виртуальная клавиатура маленькая, и пальцы задевают соседние буквы. Увы, злоумышленники об этом тоже знают и создают специальные программы, которые позволяют перебирать в автоматическом режиме все комбинации и создавать фальшивые сайты.

Например, если вместо «Сбербанк» написать «Сбербамк», то можно попасть на сайт интернет-кредитов, который к «Сбербанку», понятное дело, не имеет отношения. Или это может быть сайт, похожий на «Сбербанк» по интерфейсу, который предлагает логин и пароль к онлайн-банку.

Во-первых, надо внимательно смотреть на то, что написано в строке браузера, а во-вторых — использовать специальный инструментарий браузера, который позволяет блокировать фишинговые ресурсы (блокировщики скриптов и рекламы — см. предыдущий пункт).

**5. «Когнитивные» пароли**

Нельзя использовать один и тот же пароль для доступа к совершенно разным ресурсам, как корпоративным, так и личным. Очень многие пользователи из года в год совершают одну и ту же ошибку: меняют в пароле 1-2 символа в конце или начале, но его основу оставляют прежней.

Чтобы сделать разные пароли к разным сайтам и не забывать их, во-первых, можно использовать password-менеджер, а во-вторых, придумать алгоритм выбора паролей. Например, существуют так называемые «когнитивные» пароли, когда мы используем в качестве пароля не номер паспорта, не дату рождения, не имя питомца, а ассоциацию либо, скажем, первые две или три буквы любимого стихотворения или песни. С одной стороны, такой пароль трудно взломать, но с другой — вы его легко вспомните, когда это понадобится. Ведь тут надо помнить не саму комбинацию, а то, что вам нравится. Киберпреступники активно пользуются словарями паролей, но ваша личная ассоциация вряд ли в них содержится.

Сложность — а значит, и уровень безопасности — пароля в большей степени определяется его длиной, чем конкретным набором. Хотя, конечно, добавление специальных символов, использование и символьных, и строчных букв, и цифр тоже усложняет кодовое слово.

**6. Угроза из-за плеча**

Злоумышленники часто пользуются невнимательностью пользователей и подсматривают логин и пароль, которые те вводят в общественных местах. Защититься от этого можно, если использовать специальный экран, который защищает от подсматривания со стороны — своего рода «лист», который прикрепляется к смартфону с помощью липучек и позволяет видеть экран только вам.

А вот заклеивать камеру на ноутбуке особого смысла нет. В массе своей киберпреступники этим не пользуются. Технически слежка возможна, но ее вероятность мала: что особенного увидит злоумышленник? А следить 24 часа подряд за тем, что происходит в видеопотоке — это слишком дорого обойдется.

Даже смарт-телевизоры — теоретически более опасная штука, особенно если телевизор стоит перед кроватью: тогда там можно увидеть гораздо больше. Но на практике и такая слежка если и встречается, то очень редко. Это же касается и взлома других подключенных к интернету устройств — автомобилей, кардиостимуляторов, кофеварок. Да, это возможно, но этим никто из киберпреступников не занимается, им это попросту не нужно: есть более простые пути. Возможно — в будущем, но не сейчас.

**7. Доверяй, но проверяй**

В сфере безопасности доверие — это именно та точка, где начинается провал. Сейчас среди специалистов по безопасности широко распространена концепция Zero Trust Security — «безопасность с нулевым доверием». Мы изначально исходим из того, что никакого доверия быть не может, и протоколы и программы рассматриваем, исходя из того, что против нас действует враг, он может подменить кого-то, выдать себя за кого-то и т.п. Подобную стратегию я рекомендую и обычным пользователям. Конечно, это работает далеко не всегда: ведь человеку свойственно доверять, а киберпреступники пользуются этим. А если не доверять никому, то жить становится неинтересно, грустно и тяжело.

**8. Какие книги помогут понять психологию хакеров и характер киберугроз**

Клиффорд Столл, «Яйцо кукушки». Роман об американском специалисте, который рассказывает, как поймал одного из самых известных хакеров мира. Основано на реальных событиях. Автор объясняет, как работает специалист по безопасности, насколько это в действительности нудная работа, требующая большой внимательности.

Кевин Митник, «Искусство обмана». Автор рассказывает о том, как сам был когда-то хакером, обманывал людей, втирался в доверие, крал данные и взламывал системы, а также объясняет, как с этим бороться. Это взгляд с двух сторон: со стороны хакера и со стороны специалиста по безопасности, которым Митник впоследствии и стал.