Как сделать ваш смартфон максимально безопасным:

Технология составления паролей

Многие владельцы смартфонов ошибочно считают, что никакой суперважной информации в их телефонах не хранится. В то же время смартфон, если его не защитить, способен предоставить злоумышленникам доступ к персональной почте пользователя или аккаунтам в социальных сетях. В итоге в руки преступников могут попасть пароли, например, от онлайн-банкинга или учётной записи в платёжной системе или интернет-магазине. А это уже может привести и к прямым финансовым потерям.

Что делать в этом случае владельцу смартфона? Для начала перед тем, как обращаться в полицию, необходимо до утери аппарата знать персональный серийный 15-значный номер телефона, который высветится на его экране после набора комбинации *#06# и который надо зафиксировать.

Если на устройстве заранее установлены программы, позволяющие заблокировать доступ к телефону, то ими надо немедленно воспользоваться. Если телефон всё же утерян, то ещё до написания заявления в полицию стоит сразу же заблокировать SIM-карту и поменять все пароли от персональных онлайн-аккаунтов.

Основным рубежом для злоумышленников является пароль, установленный на смартфоне.

Технология составления паролей

Уже несколько лет американская компания SplashData, выпускающая приложения для защиты информации в мобильных устройствах, собирает статистику о том, какие пароли используют пользователи в Интернете. По результатам исследования сотрудники SplashData ежегодно составляют список «25 худших паролей».

По итогам 2013 г. среди них появился лидер - сочетание цифр «123456», которое вытеснило слово password («пароль») на второе место. Третье место заняла комбинация «12345678» (возможно, пользователи считают её более сложной для подбора, чем цифры от единицы до шестёрки); четвёртое и пятое места достались сочетаниям букв qwerty и комбинации «abc123».

В десятке худших - паролей 2013 г. также можно встретить сочетание цифр «123456789» и «1234567»; пароль, состоящий из шести единиц, фразу iloveyou и «adobe123».

Так как же следует грамотно составлять пароли? **Во-первых**, пароль должен быть не менее чем из восьми символов (лучше более десяти) и обязательно содержать как буквы (прописные и строчные), так и цифры и другие символы (при этом его стойкость к взлому многократно возрастает).

Во-вторых, пароль должен быть абсолютно неочевидным для преступников. Например, можно

взять страницу из «Витязя в тигровой шкуре», выбрать из слов последние правые буквы строк и расставить между ними цифры, составляющие год рождения любимой девушки. Получится что-то вроде «о1к9у9р4Е».

Если добавить в конец пароля, например, знак «#», то никакой прямой перебор символов за обозримое время не поможет злоумышленнику взломать пароль.

При этом надо помнить, что никаких осмысленных логически связанных слов в составе пароля не должно быть в принципе.

Если пароль кодируется цифрами, то для его запоминания (по рекомендации одной российской фирмы) следует иметь в виду, на что похожи цифры (когда включаются ассоциативные связи, то понятие лучше закрепляется в долговременной памяти):

0 - это шар;
1 - ручка;
2 - лебедь;
3 - наручники;
4 - парусник;
5 - беременная женщина;
6 - головастик;
7 - бумеранг;
8 - снеговик;
9 - теннисная ракетка.

Чтобы запомнить, например, пароль 429806, можно представить, что вы стоите на палубе парусника (4), и тут прямо на вас летит лебедь (2). Вы ударяете его ракеткой (9), он превращается в снеговика, а после второго удара шаром (0), снеговик превращается в головастика (6).

Наконец, **в-третьих**, целесообразно использовать как можно больше различных паролей. К банковскому счёту - один, к электронной почте - другой, к социальным сетям - третий и т.д.

Если таких паролей много, то запомнить их все, конечно, сложно. Как утверждают психологи, до пяти понятий, цифр, паролей и т.п. достаточно легко запоминаются обычными людьми (не зря пин-код банковской карты включает четыре цифры, чтобы его запомнили даже пожилые люди); до семи - требуется уже незаурядная память человека, а девять и более понятий и т.п. запоминают, как они утверждают, уже люди с элементами гениальности.

Когда количество используемых паролей больше пяти, то следует организовать специальный файл этих паролей на компьютере, которые в нём надо хранить зашифрованными хотя бы с помощью средств Microsoft Office.

Этот файл необходимо запаролировать с учётом всех вышеуказанных рекомендаций (как раз в этом случае особо желательно, чтобы длина пароля была более десяти символов), присвоить этому файлу имя, например, TableTextServiceYZ с расширением *.txt и поместить его в папку TableTextService в составе раздела Program Files в Microsoft Office (т.е. имя файла паролей должно быть близким к именам других файлов в папке). Чтобы окончательно запутать злоумышленника, дату создания этого файла необходимо сформировать близкой к датам создания других файлов в папке TableTextService.

Источник: Арутюнов В. В. Вы внимательны? «Злые птички» не дремлют! / В. В. Арутюнов // Современная библиотека. – 2014. - № 4. - С.22-27.

Подготовлен Мысиной Е.С.,
начальником ИЦОД,
тел. 74-00-91,
aqua@libnvkz.ru