

# КАК ЗАЩИТИТЬСЯ ОТ КРАЖИ ПАРОЛЕЙ?

В последнее время участились случаи кражи паролей dial-up и POP3 для доступа в Интернет и к почте.

## ИСТОЧНИКИ УТЕЧКИ

Главные источники опасности это:

- знакомые и сослуживцы, имеющие доступ к вашему компьютеру;
- "троянские кони" - программы, имеющие некоторые дополнительные функции;
- записи паролей оставленные на видном месте.

Также утечка паролей может быть и не со стороны пользователя.

Windows имеет далеко не совершенную систему шифрования паролей, на сегодня можно со всей уверенностью заявить, что пароли в Windows практически открыты для чтения. Существует множество программ, позволяющих читать пароли. Это и расшифровщики файлов \*.pwl, и программы, показывающие, что скрывается за знаками \*\*\*, наконец, шпионы записывающие все нажатые клавиши.

Допуская к компьютеру посторонних людей, всегда помните, что для того, чтобы переписать пароли, достаточно нескольких секунд. Не пользуйтесь своими паролями на чужих машинах.

"Троянские кони" чаще всего выдают себя за "честные" программы, попав на компьютер, они могут один раз выполнить свои действия и самоуничтожиться или остаться на компьютере и передавать сведения при каждом подключении к сети.

Сейчас широко распространилось явление, когда такие программы засылаются почтой. Не запускайте программ, полученных вместе с письмом, если только вы сами не попросили их прислать.

Прежде чем переписать новую программу, поищите ее на известных сайтах (например, Tucows), как правило, там нет "троянов" и вирусов, а если такое и случается, их быстро выявляют.

Записанный на клочке бумаги, пароль может попасть на глаза человеку, который в последствии им воспользуется. Идеальный пароль, это пароль, который, во-первых, невозможно подобрать перебором известных слов и чисел, а, во-вторых, легко запоминается.

Лучше, если такой пароль будет состоять из двух несвязанных между собой частей, например - 'палый' и '4/3'. Если его набрать большими и маленькими буквами, то выглядеть он может следующим образом: пАЛый4/3; если набрать на латинском регистре - gFkq4/3. Такой пароль практически невозможно подобрать, но легко запомнить.

## РАБОТА В СЕТИ

Прежде чем воспользоваться услугами того или иного сайта в Интернете, посмотрите, как реализована на нем защита паролей. "Дыркой" в защите часто является сообщение пользователю забытого пароля. Например, забытый пароль часто высылается по почте на указанный при регистрации адрес. На сайтах, бесплатно регистрирующих адреса электронной почты, ящики часто ликвидируют, если на них несколько месяцев не приходит почта, соответственно, вновь зарегистрировав такой ящик, злоумышленник может узнать ваш пароль на другом сайте. На некоторых сайтах забытый пароль можно узнать, сообщив дополнительную информацию. Эту информацию пользователь пишет при регистрации и, как правило, она защищена хуже, чем сам пароль.

Часто пользователи, заполняя анкету для получения электронного адреса, пишут правду и, если знать данные владельца, можно легко получить заветный доступ. Заполняя анкеты, старайтесь не писать верные данные, пишите, например, что вы из Албании и зовут вас Бил Коль.

Отдельный случай утечки это те "дырки" в защите, которые вы не можете знать. Например, несовершенство процесса регистрации, старое программное обеспечение на сервере, ошибки админов. Здесь вы, к сожалению, ничего не можете сделать.

## ГДЕ ХРАНИТЬ ПАРОЛИ В WINDOWS

*Никогда не храните пароли в скриптах, даже если они переименованы.*

**Сотрите** файл \*.pwl и запретите его создание. Обычно этот файл (их может быть и несколько) находится в папке **C:\WINDOWS** (для поиска выполните "Пуск" -> "Найти" -> "Файлы и папки" -> введите \*.pwl в поле "Имя" -> нажмите кнопку "Найти"). В этом файле хранятся все пароли, в том числе и от Internet'a. Лучше их вообще не хранить, а набирать каждый раз вручную, но, если это вызывает лишние трудности, воспользуйтесь для дозвона и получения писем нестандартными программами, которые шифруют пароли по своему собственному алгоритму и хранят в своих файлах.

Стандартные программы плохи тем, что места хранения паролей давно известны, и украсть их несложно.

Ища нестандартные утилиты не переписывайте их с неизвестных серверов, там вам в нагрузку могут подложить "троянского коня", воспользуйтесь лучше глобальными download сайтами.

Если это возможно, проверяйте где и в каком виде программа хранит пароли. Программа дозвона EDialer, например, сохраняет пароли в файле EDIALER.INI, который находится в каталоге Windows. Если злоумышленник похитит этот файл, то ему даже не надо будет пытаться их расшифровать - он просто подложит его своей копии EDialer.

Полагаться на Windows - это значит полностью открыть пароли для чтения (почему, см. выше). Значит,

**единственный способ обеспечить безопасность в этой программе – это набирать каждый раз пароль вручную.**