



Name: Advanced Office XP Password Recovery

Version: 2.30 – Professional Edition

Supplier: ElcomSoft

Price: US\$150 / £97.46

URL: <http://www.elcomsoft.com/>

Platform: MS Windows 95, 98, ME NT4, 2000 and XP

System: Pentium Processor, 32mb RAM, 15MB hard disk space

The Advanced Office XP Password Recovery tool is one of those tools you'll never think of buying until the day comes when you can't do without it. The day the password is forgotten or the day the guy with the password to that important sales proposal or next year's financial plan leaves. That's where the Advanced Office XP Password Recovery (AOXPPR for short) tool comes in.

This tool has a clear aim of cracking passwords set on things like word documents, excel spreadsheets. Apparently a favourite of the "FBI" this tool features a number of well known password recovery techniques to try and recover or crack the password on that all important file.

AOXPPR recovers lost or forgotten password for the following applications including all versions up to 2002/XP.

Microsoft Word	Passwords to open and modify and document protection passwords.
Microsoft Excel	Passwords to open and modify, workbook passwords including shared workbooks, sheet passwords.
Microsoft Access	Share-level passwords, database owner information (user name and securityID) and user level passwords for system databases.
Microsoft Project	Passwords to open and modify.
Microsoft PowerPoint	Passwords to open
Microsoft Outlook	Passwords to open PST files, password for email accounts

This program also has VBA "Backdoor" features which works for all Microsoft 97, Office 2000 and Office XP applications as well as some other projects which have VBA projects built into them such as Money, Backup, Schedule+ etc (see the website for full details).

Purchase of the program can be made online and couldn't be easier. During purchase the program can be downloaded. Once payment has been made a registration code/serial number, which converts the download into a fully functional version, will be emailed to the buyer.

Both the documentation and support of the product is very good although the odd word has been badly translated. The company website is very good and it has free updates posted for the product.

As for usage the tool has two main modes for guessing passwords.

The Dictionary Attack used by this tool takes a file that contains a number of plain text words such as "apple", "Fred", "window" and so on and uses each word in turn to try to access the file to see if it is the lost/misplaced/unknown password. If the usage is successful and the correct word is found a notification will be given to the user.

A dictionary file comes complete with the tool. The file contains over twenty-five thousand words which may seem like a lot until I tell you there are free dictionary files you can download and install that contain over eight million words.

This method of attack relies on the original user, the one who set the password, not using correctly constructed passwords. It assumes they used a simple, plain text word. Very often this method of attack will pay off so it's worth trying this method of recovery first.

The Brute Force Attack is a far more complex attack. You give it a number of parameters such as minimum and maximum (or as the poor translation puts it Minimal and Maximal ☺) password length, the types of characters (upper/lower case, spaces, punctuation and even custom character sets) and even allows masks if you know a portion of the password such as "happ*".

This type of attack attempts to break well constructed passwords by producing thousands and thousands of different passwords to try based on the preferences you select trying each one in turn.

This works very similar to trying to break a 4 digit pin code by trying 0000 then 0001 then 0002 and so on until you run out of possibilities at 9999. Now as you can imagine this takes time especially when you state an 8 character password that could be made up of anything from 26 lowercase letters, 26 uppercase letters, numbers, special characters, characters of another language etc. Now if you know part of the password and can use the mask feature this is going to reduce the processing time.

Anyway you look at it though if a password is well constructed it will take a lot of time and a lot of processing power even if the tool can generate and check passwords at over 235,000 passwords per second or so the inbuilt benchmark checker tells me.

My Verdict:

This is a very specific tool for a very specific task and you might only ever need to use it once which makes the price tag hard to swallow.

One major problem with this tool though is the speed when using brute force passwords cracking. Although optimised and very quick it still takes a lot of computing power and a long, long time to crack a well constructed 8 character passwords. Thankfully most users do not use well constructed passwords!

All in all it is possibly the best all round password recovery tool I've come across for the Microsoft platform and given enough computing power and time will crack any lost password on compatible files.

Rating	
Features	3/5
Ease of use	4/5
Performance	4/5
Documentation	3/5
Support	4/5
Value for Money	3/5
OVERALL	3/5

PRO

- Simple and easy to use
- Good features

CONS

- The supplied dictionary for password guessing is quite small.
- It can take a long time to brute force a well constructed password even with powerful computers