Copyright and Disclaimer

WinWord Password Recovery Tool

Windows 95/NT 4.0 Edititon

Version 1.5

Revision Date: January 1998

WARNING

Disclaimer

The developers and distributors of WWPRT make no warranty of any kind, either express or implied, with respect to this software and accompanying documentation. In no event shall the developers be liable for any damages arising out of the use of or inability to use the included programs. The e ntire risk as to the results and performance of this software package is assumed by the customer. We specifically disclaim any implied warranties of merchantability or fitness for any purpose. Use at your own risk.

The developers and distributors of WWPRT reserve the right to revise the software and accompanying documentation and to make changes in the contents without obligation to notify any person of such revision or changes.

What is WWPRT

WWPRT stands for **W**in**W**ord **P**assword **R**ecovery **T**ool. It allows forgetful users to find out what password they used to protect their documents. The current release works only on Word 6 and 7 documents. WWPRT is a 32-bit program and it requires Windows 95 or NT 4.

We wrote WWPRT because there seems to be a need for this sort of tool. There are some other products that claim to do password recovery, but their price tag is in the $180-$300 range. We do not exactly understand why they are so expensive. WWPRT is a simple tool that does one thing, and does it very well. We are asking for **$37** for the program and a few bucks for shipping and handling. **If you forget the passwords to your documents, or you are involved in a tech support or help desk position that requires you to deal with people who forget their passwords, then WWPRT is just the tool you were looking for. It is simple to use, it works faster than blink of an eye, and it is inexpensive.**

In addition, WWPRT has a nifty feature. It can attempt to discover the correct password by trying out a range of values. The user can designate which characters should be checked by entering the value **FF** in the proper position. After setting the range of characters to try, one click on the Try button sets WWPRT on its way to brute-forcing every combination until a potential hit is discovered. To see this in action, just replace a few characters even though WWPRT has found the correct password. After the search, you should get back the correct values again. Only up to 3 characters are searched for. The reason is quite simple: On a Pentium PC, it takes under 3 minutes to check all possible combinations. If we set that limit to 4, it takes over half an hour. If we set it to 5, it takes 29 hours, and so on. Brute-force search should not be necessary in most cases you are likely to encounter. The correct password is found and displayed as soon as you select a document in most cases.

WWPRT does not decrypt files. If the document is not password protected but there's an edit protection on it, then WWPRT modifies the document only if you allow it to remove edit protections. Otherwise, it simply reads the relevant parts of a Word document, and using simple cryptanalysis methods, it computes the encryption key and and the potential password used to generate it. After the password is found, you need to enter it into WinWord's password box when you are prompted. This should unlock the document for you. If there are edit protections after Word unlocks the document, then you can run WWPRT on that document again to remove them as well.

Program Requirements

WWPRT requires the following:

- Windows 95 or NT 4 or better
- OLE2 DLLs (included in Windows 95 and NT 4)
- 120K disk space

WWPRT supports the following document formats:

- Word 6
- Word 7 or Word for Windows 95 32-bit edition

Formats NOT supported:

- Word 8 or Office 97

Fequently Asked Questions

- **How does WWPRT work?**

Very well actually ;-) We have analyzed the WinWord program and the algorithms it uses to encrypt documents. Based on that analysis, we were able to design a simple cryptanalytic attack against the encryption scheme WinWord uses. It turned out that there are inherent weaknesses in the scheme that product uses.

- **What kind of encryption does WinWord use?**

WinWord uses what is called a polyalphabetic substitution cipher with a period of 16. Basically, Word takes the password the user entered, pads it out to 15 bytes if it is too short, and generates a 16-byte encryption key. It then uses the XOR operation to encrypt each byte in the data portion of the document 16 bytes at a time. It also stores two checksum values in the document header so that the password can be verified when the user wishes to open the document later. If the verification is successful, it uses the same operation to decrypt the document. To reduce the possibility of giving away the encryption key, it also skips over values that match certain criteria. It does not store the password anywhere in the file.

- **Am I allowed to use WWPRT on my home computer?**

Absolutely. Once you buy a copy of WWPRT, you can use it on as many computers as you own.

- **Who needs WWPRT?**

Many WinWord users who password protect their files for privacy reasons. Humans often forgets passwords. This is a well-known fact. In addition, tech support personnel may find it useful if people in their company forget the passwords to documents they have created in Word.

- **Does WWPRT work on Word 8 documents?**

The current version does not handle Word 8 binary format which is used in MS Office 97.

- **What if it cannot find the password?**

This is possible but quite unlikely to happen. If it does happen, there may be something wrong with the document you are trying to break. To make sure, you can send us the document for analysis and we will try to retrieve the password manually for you. If it turns out to be due to a bug in WWPRT, we will look into it and send you a free update as soon as one is available.

- **Does WWPRT remove edit protections?**

Yes, it can. If the document is password protected (cannot even open without a password), then you first need to obtain the password from WWPRT, enter it in Word and open the file. Then save the file without a password. After that, you need to run WWPRT again to remove the edit protections. If the document was not password protected but had only edit protections, then WWPRT will clear them when you first run it on the document. You will be asked if it should do so.

- **Is WinWord encryption secure enough for common use?**

The encryption scheme Word uses is difficult enough to deter a casual user from manually recovering the key or the password. However, somebody trained in cryptanalysis can break it fairly easily. As you can see, WWPRT finds the password before you can blink an eye. If you wish to have stronger protection for your documents, then you should consider other products that supplement Word's encryption.

- **How do I know you are not cheating?**

Because we allow you to test drive WWPRT. You can create a document in Word and protect it with a password of 12 characters. Then you can see if WWPRT can discover the password. There is nothing magical about the number 12. We chose it arbitrarily; it's long enough to make a brute-force search infeasible.

- **Which language is WWPRT written in?**

WWPRT is a 32-bit Win32 program written in the C language. Certain sections of the code are written in hand-optimized ASM for speed. WWPRT is based on the **StripSearch(tm)** technology we have developed to be able to scan and disinfect password protected documents. Some macro viruses can also encrypt document with random passwords. Our antivirus product, **Perforin for WinWord**, also uses **StripSearch(tm)** technology. You can get a trial copy of Perforin from our website at **http://www.vdsarg.com**.

- **How did you test WWPRT?**

This was the tricky part. We put together a test program that can generate password protected Word documents on demand. We then ran it with random passwords with sizes varying from 1 to 15. For each password length, we tried WWPRT against thousands of documents. It passed with flying colors. Then we sent it to a few trusted beta-testers, and they liked it as well.

- **What if the bad guys use WWPRT to steal information?**

This is a possibility. However, if anyone is concerned about the safety or privacy of their confidential information, they should use something much stronger than Word's encryption. Besides, there are other products already available to do the same thing. We simply offer an inexpensive alternative to the people who really forget their passwords. WWPRT can also be used by law enforcement people to discover the password to documents that may hold information about criminal activities. So, it's a double-edged sword.

How to Order WWPRT

To get the fully functional copy of WWPRT, you need to fill out the order form, enclose your payment or credit card information, and mail it to our address. Orders are processed with in 1-2 weeks. **Most major credit cards are accepted**.

For faster service, you can fill out the form and email it to our address:

wwprt@vdsarg.com

Optionally, you can use the online ordering utility we include with the trial copy. You can access it under the Help menu in WWPRT as the Buy the Real Thing command. This will allow you to fill out the order form and submit it to our secure FTP area over the Internet. You must have an active connection to the Internet before you start the ordering procedure. You can also fill out the order form and fax it to (**410) 594-9208**.

Once the payment is received, we will make the full copy available to you over the Internet. Download instructions from a restricted area of our website will be sent via email. The entire package is less than 100K in a ZIP archive. We could also email it to you if your email host supports receiving binary attachments.

By registering WWPRT, you get the fully functional copy. In addition, you encourage our efforts to provide similar solutions to the user community at reasonable prices. The trial copy of WWPRT will work on documents that were encrypted with a password length of 12 characters. We set it up this way for you to test drive the program before purchase. The full copy has no such limitations. **All sales are final, and returns will NOT be accepted**. WWPRT costs only $37 plus $3 for shipping and handling in the U.S.

Order Form

VDS Advanced Research Group
PO Box 9393 Baltimore, MD 21228, U.S.A.

Fax: (410) 594-9208 http://www.vdsarg.com wwprt@vdsarg.com

WWPRT 1.5a Order Form

* All sales are final. Please download the trial copy before purchase.
* Shipping address is required for credit card verification.
* WWPRT does NOT work on Word 8 or Office 97 documents.

Date: ___/___/_____

Name:_____

Daytime Phone:_____Other Phone:_____

Shipping Address: _____

_____

City:_____

State:_____**Zip**:_____

Email address:_____

Quantity:_____ Price/Unit:_ $**37**.00

Sub-total:_____ (multiply quantity by price/unit)

Shipping:____$**3**.00_(add another $**15** if you are outside the U.S.)

Sales Tax (5% in MD):_____ (multiply sub-total by 0.06)

TOTAL:_____ (add sub-total, shipping, and sales tax)

Payment Method:

( ) Check #:_____ (payable to VDS Advanced Research Group)

( ) Credit Card:
( ) VISA ( ) Mastercard ( ) Discover ( ) AmEx

Card Number: _____ Exp. Date: _____

Name on the Card:_____

Customer's Signature:_____

-Where did you get the trial copy of WWPRT?
( ) http://www.vdsarg.com ( ) http://www.ccso.com

( ) http://www.psnw.com/~joe ( ) AOL ( ) Other:_____

-May we add your email address to our list to notify you of new releases?
( ) Yes ( ) No

* Fill in the blanks, enclose a money order (outside the U.S.) or check for the total amount and mail it to our address. Allow 1-2 weeks for delivery. You can also pay by credit card and request electronic delivery over the Internet.

==========

For us to serve you better, please answer the following questions:

1. Do you use WinWord at home? ( ) No ( ) Yes____version:_____

2. Do you use WinWord at work? ( ) No ( ) Yes____version:_____

3. Do you use any other word processing program besides WinWord?
( ) No ( ) Yes _____

4. Did you upgrade to WinWord 8 or MS Office 97? ( ) No ( ) Yes

5. What is your operating system? ( ) Windows 95 ( ) Windows NT 4

==========

* You can direct all questions/suggestions to wwprt@vdsarg.com