Using RiNGminder™ Safely and Effectively

Your new **RiNGminder**™ is designed to let you generate, and later recall, secure and difficult to guess passwords which are unique to each website or account you log into, while only having to remember one simple rule. People must maintain many passwords nowadays and it is difficult to avoid falling into the trap of using one password everywhere, or too-easy-to-guess ones.

Modern password security demands that passwords be *at least* 8 characters in length, and consist of letters (both upper *and* lowercase), numbers *and* punctuation. This makes them extremely difficult to recall of course... Using **RiNGminder**™, you gain the benefits of *two-factor security* – something you *have* (the device), and something you *know* (your secret word or words, see below).

Each ring has 26 rows of symbols – a letter paired with a number or punctuation symbol, separated by one or two dots. All letters of the alphabet, plus all digits 0-9 are on each ring.

How To Use

1. Save all included sheets! If you lose your **RiNGminder**™ use the SYMBOL SET sheet to avoid needing to change all of your passwords until a replacement arrives.

2. Make note of the order in which you pair the rings. If you remove them, you'll need to put them back in the same order. It's easiest to just make note of a row on each with the same letter. If they don't fit your fingers, you can put them on a necklace, bracelet, friendship band etc.

3. Come up with a two-part rule to dial in your **RiNGminder**™, such as (these are just examples):

Part I:

-First two letters of the website or company; or
-First and last letters of the website or company

Part II:

-A short secret phrase. Choose to add this to the start, middle or end of your dialed-in password. Capitalize at least one letter of the phrase.

Notes On Secret Words

A long-gone pet's name is... OK, but your middle name reversed is even better, or better yet a nonsense phrase... be creative. However, be sure it is NOT something you always talk about, online or in public and won't show up in a web search! Names are good since they have a capital letter as well.

Example – 'hotmail.com', secret word 'BuckleBees':
Dial in **h o** on your pair of rings (ignoring the digits or symbols beside each), then read off TWO rows of symbols BELOW this on each ring. *Don't* use the row dialed in as Part I of your password; that contains part of the word 'hotmail', which would weaken your password since it's related to the site.

Assuming the rows below **h o** on your rings now read **j% r$ u5 m2** in this position (they likely won't – each batch of rings are unique) your password for hotmail.com would now be:

j%r$u5m2BuckleBees

(While letters on the rings are in uppercase, you can choose to interpret them as lower- or upper-case; just be consistent and make the same choice for every site.)

Even if someone steals your **RiNGminder**™ or sees you dial in a password, they only know part of the secret. Remember, only you know the secret word(s) you chose and how they're added to the dialed-in symbols.

Dealing With "Stone-Age" Password Policies

Some sites only allow passwords of a limited length of 8-12 characters; or only letters and numbers; or only limited punctuation; or worst of all, all three! These are called "**Stone-Age**" (defective) password policies.

Firstly, email the site owners to improve their password policy! They reduce everyone's security. In the meantime, come up with a **fallback rule:** dial in as usual, but use a 4-letter fallback secret word, and read off just ONE row of symbols, substituting the first letter of each punctuation symbol's name – 'o' for '(' open-parenthesis, 'c' for ')' close-parenthesis, 'g' for '>' greater-than, and so on. You'll get a password that has only letters and numbers, and is 8 characters long (4-letter secret word plus 2 symbols per ring = 8 characters).

Following the example rule above, if 'hotmail' only allowed 8-character passwords with no punctuation, you'd get **jprdBees (j 'percent' r 'dollarsign' Bees)** which satisfies Stone-Age password policies. If the

policy **does** at least require numbers, which this example lacks, use the count of dots on the rings at the positions you dialed in (here, the number of dots between **j%** and **r$**) as a digit to add.

Corporate Accounts

Corporate networks commonly require password expiry: new passwords that change, say bi-monthly. For these, use the regular procedure at each renewal date, but make note of the current month (1 = Jan, 2 = Feb, etc.) and rotate the last ring by that many positions (or two, in the unlikely event that you've come around again to the same password after a year). Just make note of the month you do this each time.

Advanced Uses

Two people with a matched pair of rings can use them to exchange short messages using mono- or poly-alphabetic substitution ciphers (using the single- or double-dots on each row as shift counters). Can you think of other, even trickier ways to user them? This is more for 'fun' – but who doesn't love secret messages?

*** DISCLAIMER ***
NOTE that while the manufacturer does not endorse or support the use of **RiNGminder**™ rings for encryption purposes, they can be used as fun 'secret code rings'. BE HEREBY WARNED that the **RiNGminder**™ DOES NOT provide security against entities with sophisticated intelligence resources. BE AWARE THAT the product is sold as-is, and manufacturer provides absolutely no warranty of FITNESS FOR A PARTICULAR PURPOSE including, but not limited to, its use in securing/maintaining data and/or correspondence for the protection of economic interests, reputation, monetary assets of any kind, personal liberty or well-being. MANUFACTURER ACCEPTS NO LIABILITY for the products' inappropriate use by any party in disregard of this disclaimer.

Package Contents:
-One pair of **RiNGminder**™ rings
-Instruction sheet
-Symbol code sheet

russtopialabs.bigcartel.com
russtopialabs@gmail.com

v1.2