How Neo's SafeKeys Works

Neo's SafeKeys v3 protects you from keyloggers, clipboard loggers and screenloggers in the following ways:

Keylogger protection:

What are keyloggers?

There are two main types of keyloggers – hardware and software keyloggers.

Hardware Keyloggers are hardware-based tools that record keystrokes. They may reside within the keyboard circuitry or the keyboard casing (therefore almost impossible to detect), or a dongle between the keyboard and the computer (eg a PS2 adaptor or a USB adaptor).

Software Keyloggers are software-based tools that record keystrokes typically using your operating system to capture your key presses. There are different levels to your system that they usually work from:

- The Windows Kernel. The 'guts' of the Windows system may be infected by keyloggers. Hard to write, and really hard to combat.
- Windows 'hooks'. Windows gives the hook-based keylogger advance warning of every keystroke that is made – before it ends up on the applications.
- Passive methods. The keylogger continually 'polls' Windows to see if a key is pressed…and which key is pressed.

Software keyloggers can be installed without your knowledge and without you installing any software. All it takes is you going to a hacked website, and you could have one.

It does help for you to have a good virus checker, and some anti malware software, but even then, recent studies have shown that you can be infected by keylogging trojans…even if you have up to date anti-virus software. There is no way to be totally safe when using your keyboard.

How Neo's SafeKeys v3 provides protection:

Neo's SafeKeys v3 provides great keylogger protection.

The way it does this is simple – you don't use your keyboard to enter or manage your passwords. At all. Ever.
This is the *best* way to defeat hardware and software keyloggers.

Please note that it is safer when you do not use the injection mode – we have been informed that *some* keyloggers can pick up the injected text. However, if you use the injection mode in conjunction with a program like KeePass, you are still afforded good protection.

Clipboard logger protection:

What are Clipboard Loggers?

Clipboard logging is a common feature of trojans, viruses, keyloggers and other malware. Whatever you copy to the clipboard is stored, then transmitted to the trojan/virus 'bad guys'.

Be aware of tools that say they offer clipboard logger protection – if you can use your clipboard, then

keyloggers can also use it. In short, there is no way to protect your passwords if they are cut/pasted through the clipboard.

How Neo's SafeKeys v3 provides protection:

Neo's SafeKeys provides 100% clipboard logger protection by never using the clipboard. The clipboard isn't used in the transmitting of your passwords. At all. Ever.

Screen logger protection:

What are Screen Loggers?

Screen loggers are also a common feature of trojans, viruses, keyloggers and other malware. They used to be reasonably rare, but are becoming a standard 'feature'.

They take photos of your screen – usually just around your mouse – either at periodic intervals, or every time you do a mouse click.

There are generally three ways that screenloggers can take pictures.

1. They can remote control the Print Screen key. (This almost never happens in practice, because users will see screenshots in the clipboard or a changed/cleared/flickering keyboard, and the logger will be found out – but it is still technically possible.)
2. They programattically take a screenshot of the *control* (button, text box etc) that is under the mouse using Windows API commands.
3. They programattically take a screenshot of the *desktop* using Windows API commands. (Many can't take screenshots of transparent windows like Neo's SafeKeys – which is always at least 1% transparent.)

How Neo's SafeKeys v3 provides protection:

1. Neo's SafeKeys disables the Print Screen key whenever it's running.
2. Neo's SafeKeys v3 has a new feature to protect against screenshots being taken of controls under the mouse – an (invisible) protective layer.

What is it? It works like this:

The protective layer provides a buffer between the mouse and the Neo's SafeKeys buttons. Therefore,

when screen loggers take pictures of the control under your mouse, they're taking pictures of the protective layer – not Neo's SafeKeys buttons. The screen logger will only get a green rectangle – and no keys. This way you're protected against this second type of screenlogging.

3. Neo's SafeKeys is always at least 1% transparent. Why? Desktop screenshots taken using the more common Windows commands don't 'see' transparent windows. Neo's SafeKeys is totally invisible to viruses/trojans using these techniques…no matter if it is 30% transparent or 99% transparent.

Do note that *some* screen loggers can still take pictures of Neo's SafeKeys – they use a different capture method that is able to circumvent transparency and the protective layer. The hidden mouse mode will provide protection from these types of screen loggers.

Other Neo's SafeKeys v3 features include:

Mouse Position protection:

What is Mouse Position Logging?

Prior to screen logging becoming a standard feature, mouse position logging was sometimes used to defeat people using the on-screen keyboards on banking websites.

How does it work? Each time you click, the coordinates of your mouse are captured by the virus/trojan. Because the banking website's on-screen keyboard is the same height/width every time, the virus/trojan writer can know with a pretty good degree of certainty the on-screen keys you've clicked.

How Neo's SafeKeys v3 provides protection:

Every time Neo's SafeKeys is run it starts up in a different position on the screen and has a different height and width.

The "Resize SafeKeys" button will also reset Neo's SafeKeys' height/width and position, whenever pressed.

Protection against 'field scraping':

What is 'field scraping'?

'Field scraping' is a term we use to describe a technique used by quite a few commercial keyloggers to grab your passwords directly from the password field.

How does it work? Using Windows API commands, programs can ask Windows for a list of controls in a program (like buttons, text boxes and picture controls). From this, they know about the text boxes in the program. They then ask Windows whether the text boxes have a password mask (ie if there is a password hidden by '****' askerisks).

Here's the scary part – they can even get Windows to give them the password – *behind the '****' password mask*.

How Neo's SafeKeys v3 provides protection:

Neo's SafeKeys <u>never</u> stores your real password behind the '****' password mask. It keeps your password safely locked away 'behind the scenes'. Keyloggers/viruses/trojans will only ever get a list of '*' asterisks.

Other Features:

Drag and Drop passwords

Neo's SafeKeys transfers your password when you drag and drop the password from Neo's SafeKeys to a destination program (eg. Internet Explorer).

As you are not typing your password, you are not using the clipboard or cut-paste methods, keyloggers cannot capture your password during the dragging and dropping process. In short – we have not seen any keyloggers that are able to capture dragging and dropping. We don't even know how it could possibly be accomplished.

NEW – 'Injection' mode

Some programs don't accept dragging and dropping – these include some great programs like KeePass, Roboform, Opera, Excel and World of Warcraft.

However, Neo's SafeKeys v3 now has an 'Injection' mode, which allows you to move your passwords to these programs, in a drag-and-drop manner, quite safely.
Please note that it is safer when you do not use the injection mode – we have been informed that *some* keyloggers can pick up the injected text. However, if you use the injection mode in conjunction with a program like KeePass, you are still afforded good protection.

Different password entry methods

As you'll see, there are a few ways you can enter your passwords using Neo's SafeKeys:

- **Standard Entry** – click the on-screen keyboard buttons to register your password, prior to drag-drop to the target program.
    - Protection: Great.
- **Hover Entry** – hover your mouse over the on-screen keyboard buttons to register your password.
    - Protection: Brilliant.
- **Hidden Mouse and Hover Entry** – your mouse will be turned into a little grey dot while you hover your mouse over the on-screen keyboard buttons to register your password.
    - Protection: Insanely High.

Password and Visible Text

If you wish, you can use Neo's SafeKeys as a portable 'notepad'. If the Password Mask is disabled, you'll be able to see whatever you enter – but you could use Neo's SafeKeys to write a short note using the on-screen keyboard or a scrambled keyboard. This should afford you some protection for the notes you write

Configurable On-Screen Keyboard Layout
Neo's SafeKeys can import new on-screen keyboard layouts. You can create your own.
You'll notice that Neo's SafeKeys v3 will save your settings (but NOT your passwords) in a NSKconfig .ini file. Create a copy of this file (with a new name), and then edit this file.
The buttons are ordered by row, left to right, lowercase and uppercase. Simply replace the characters you wish to change, then import using the option on the "Keyboard Layout" menu.
If you send us an email of a particular language layout, we're happy to place this on the site for other people to use.

What the toolbar buttons are:

Mouse Entry Features:

 **Standard**

Using this mode, use the mouse to click the on-screen keys to enter passwords.

 **Hover Entry**

Using this mode, hover the mouse over the on-screen keys for a period of time to enter passwords. The hover entry delay can be set – between 500 ms (0.5 seconds) and 2500 ms (2.5 seconds).

Some keyloggers take screenshots every time you do a mouse-click. Use this mode to defeat this keylogging method.

 **Hidden Mouse and Hover Entry**

This mode changes the mouse cursor to a small grey dot. Using this mode, hover the grey dot mouse over the on-screen keys for two seconds to enter passwords. The hover entry delay can be set – between 500 ms (0.5 seconds) and 2500 ms (2.5 seconds).

Some keyloggers take screenshots at periodic intervals (whether you click anything or not);
this mode 'hides' the mouse when you have it over the on-screen keyboard.

This mode also will help protect you against "shoulder surfing" (people looking over your shoulder to see what you click).

Options:

 **Injection Mode**

With this, you can use Neo's SafeKeys v3 with programs that do not usually accept drag-drop – this means that you can now be protected when entering master passwords for KeePass and Roboform, and when using Opera, Excel, World of Warcraft and others.

 **Beep on hover entry**

When using 'Hover Entry' or 'Hidden Mouse and Hover Entry' modes, the computer will beep when an on-screen key is registered.

 **Keep password after drag-drop**

If this is enabled, all text in the password box will remain after it's been dragged and dropped to another application.

If this is not enabled, the text will be cleared after every drag-drop.

View:

 **Password Mask**

This feature toggles the password mask. If the Password Mask is enabled (default), your password is hidden behind * characters.

For example, if your entered password is “password123!”, the Password Mask is enabled, you’ll see “**********” in the password field. If the Password Mask is disabled, you’ll see “password123!”.

Obviously, it is not very secure to have the Password Mask disabled; field scrapers can grab your password.

However, if the Password Mask is disabled, Neo’s SafeKeys will register tab key presses and enter key presses. This way you can potentially type a small memo using just the on-screen keyboard.

(If the Password Mask is disabled and you have more than one line in the password field, and/or a tab character…then you enable the Password Mask, the following will occur: Neo’s SafeKeys will discard all text but the first line, it will also discard any tab characters, then will hide the remaining text behind the * characters.)

Transparency

For convenience, you may set the transparency of Neo’s SafeKeys – from 30% transparent to 99% transparent.