VIRTUAL KEYBOARDS: PROTECTION AGAINST HARDWARE KEYLOGGERS

What Are Virtual Keyboards?

Virtual keyboards are on-screen input tools that allow users to enter text by clicking keys with a mouse or tapping on a touchscreen, rather than using a physical keyboard. They are widely used as a security measure to help bypass hardware keyloggers, which are physical devices or malicious software designed to record keystrokes from traditional keyboards.

How Virtual Keyboards Protect You

- **Bypassing Hardware Keyloggers:** Since virtual keyboards do not rely on the physical keyboard, hardware keyloggers attached to the keyboard cable or port cannot capture inputs made via mouse clicks or touchscreen taps.
- **Protection Against Some Software Keyloggers:** Many software keyloggers are designed to intercept keystrokes from physical keyboards. Using a virtual keyboard can help prevent these from logging sensitive information, such as passwords.
- **Added Security Features:** Some virtual keyboards offer dynamic layouts (randomizing key positions) or keystroke shuffling, making it even harder for sophisticated malware to map mouse clicks to specific characters.

LIMITATIONS

- **Screen Capture Malware:** Advanced malware can take screenshots or record screen activity, potentially capturing your inputs on a virtual keyboard.
- **Not Foolproof:** While virtual keyboards are effective against hardware keyloggers and many basic software keyloggers, they are not a complete solution. For maximum security, combine their use with anti-malware tools and good security practices.

EXAMPLES OF VIRTUAL KEYBOARD TOOLS

TOOL/SOFTWARE	NOTABLE FEATURES
Windows On-Screen Keyboard	Built into Windows OS, accessible via Start Menu

east-tec SafeBit Virtual Keyboard	On-screen keyboard with optional key shuffling for extra protection
Kaspersky Secure Keyboard Input	Part of Kaspersky security suite; protects sensitive fields in browsers
Bitdefender Safepay Virtual Keyboard	Used in secure browser for online banking/shopping
Panda Dome Virtual Keyboard	Available in Panda security suite for safe password entry
KeyFlare	Dynamic layout that randomizes key positions to thwart screenloggers

Best Practices for Using Virtual Keyboards

- Use virtual keyboards especially on public or shared computers where the risk of hardware keyloggers is higher.
- Prefer virtual keyboards with dynamic layouts or key shuffling for enhanced protection.
- Combine with anti-malware software and keep your system updated to defend against screen-capturing malware.
- Avoid entering sensitive information on untrusted or compromised devices, even with a virtual keyboard, if possible.

SUMMARY:

Virtual keyboards are a practical defense against hardware and many software keyloggers, especially in high-risk environments. For optimal security, use them alongside comprehensive cybersecurity measures and remain vigilant about emerging threats.