Scam of the Week: Bad Guys Teach You How to Enable Macros

One of the most common ways that bad guys sneak malware onto your computer is through macro-enabled Excel files. A macro (short for macroinstruction) is a set of commands that automate a process in Excel. When you open an Excel file that includes macros, you'll see a security banner with the option to activate macros by clicking "Enable Content". Typically, malicious Excel files are attached to a phishing email. If you choose to open the attachment and enable macros, the file will automatically install the cybercriminal's malware.

In a recent phishing attack, the macro-enabled Excel attachment is designed to look like a Windows Defender help page. The spoofed help page provides easy-to-follow instructions on how to click the "Enable Content" button. To establish additional credibility, the file includes logos of well-known security vendors like McAfee. If you fall for this trick and enable macros, a dangerous piece of malware is installed onto your computer and cybercriminals will have complete access to your system.

Follow these tips to stay safe:

- Never download an attachment from an email that you weren't expecting.
- Don't let your eyes deceive you. Bad guys use familiar logos from real businesses to appear more legitimate.
- Before enabling macros for an Excel file, contact the sender using an alternative line of communication—such as by phone or text message. Verify who created the file, what the file contains, and why macros are necessary.

Stop, Look, and Think. *Don't be fooled.*
The KnowBe4 Security Team
KnowBe4.com