

## Changes to Facebook Page APIs == New Risks for Customers

*By Evan Robert Keiser, Security Analyst, Perimeter E-Security  
with Andrew Jaquith, CTO, Perimeter E-Security*

Facebook recently announced that it has implemented changes to the way a Facebook page can be created. The primary change is that Facebook pages now allow authors to use IFRAME tags in their pages. Previously, authors used Facebook's custom point and click creation interface. They were also able to create custom Facebook apps that fetched external data from third parties for display on the page. This content was fairly protected because it was all proxied through Facebook. This caused potentially malicious Java and Flash exploits not to function.

So why is this change so important to your security?

Simple: IFRAMEs are evil. And because IFRAME tags can now be included in Facebook apps, proxying can now be circumvented. This is very good news for malware writers and other cyber criminals because social engineering is no longer required to convince users to navigate to a malicious website. Instead, they can enlist Facebook to help them in their efforts.

For example, it is now possible to set up a default Facebook page, create a profile (the one you first see when you visit a user's page) and include an app with an IFRAME that contains malicious JavaScript to redirect users to arbitrary websites without any interaction required. This technique is already being used in the wild, to forward users to malicious websites.

Facebook has been informed of the security risks associated with their new feature by our colleagues at Trend Micro, though they have not received a response from Facebook yet.

In the meantime, security conscious customers should consider limiting access to Facebook. Perimeter E-Security Managed Security Service (MSS) customers who use web content filtering can easily put a rule in place blocking access to Facebook URLs