New Facebook Threat

By Denise Richardson

Love it or hate it, Facebook has become a major part of life for many. Unfortunately, whenever anything becomes as popular as Facebook is there are always going to be new scams and identity theft tactics developed to take advantage of it. The most recent threat is a revamped version of an existing tactic that thieves can use to steal the credit card info of unsuspecting Facebook users.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
  var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
  po.src = 'https://apis.google.com/js/plusone.js';
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

The new threat comes in the form of malware that injects a small amount of web code into the user's browser when it detects someone logging in to Facebook. The code creates a fake Facebook permissions window like those that users see when installing new apps or accessing other Facebook features. The window says that the user needs to verify his account and asks for a valid credit card number for this purpose. Once the number is entered then the user can proceed to Facebook without knowing that his credit card number has been sent to the malware's creator.

Scams like this aren't anything new, though the specific method used to perpetrate this one changes things up a bit. Most "verification" scams occur via email, with spoof emails from places such as eBay or other major websites saying that they need passwords, bank account information or other financial data to verify purchases, fraud claims or the user's account in general. Some of the fake emails can be very convincing, coming from spoofed email addresses that seem legitimate and containing the same graphics and wording that would be used in legitimate emails.

As always, I'll caution you to be very careful in regard to your personal and financial information. Never give out your

credit card number for "verification" purposes on websites such as Facebook; the most that these sites will ever ask for is a cell phone number that they can send a verification text to. You should also never give away your passwords or banking information in response to any email, and don't blindly follow links asking you to log in and verify your account.

If you ever receive a questionable email that asks for your password on eBay, Facebook, PayPal or other sites, don't respond to it and don't follow any links that it might contain. Visit the actual website by typing in its URL and log in to your account. If action is needed on your account you should be prompted from within your account. Contact the site's customer support team with questions about suspicious emails as well so that they can try and track down the scammers who send out the spoofs.

Should you encounter popups on Facebook or other sites asking for your credit card number or other information, run an in-depth virus scan and malware scan on your computer. You should have antivirus programs running scans regularly anyway, but additional scans when you notice strange things occurring on your computer can help you detect and protect issues sooner than later, and help keep you from becoming a victim of credit card fraud or identity theft

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow ACCESS