FTC Issues Warning about Scam to Hijack Your Email Account

July 2, 2015 â€“ The FTC has issued a fraud alert to warn consumers about a scam that is designed to hijack their email accounts. If the people behind the scam can determine both your actual email address and your cell phone number, thatâ€™s all they need to target you.

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 scam works like this. Letâ€™s say you have an email address from Googleâ€™s Gmail service. The scam artist goes to the Gmail website, putâ€™s your email address into the box to log-in and then clicks on the link provided for people who have forgotten their password and asks that a new password be sent via text message. Then the scammer sends you a text message that appears to come from your email providerâ€¦ in our example, Googleâ€¦ and asks you to respond with the password provided. If you do, then you have just turned over access to your email account to someone else.

Anyone receiving text messages like those mentioned above should not respond to them. And anyone who thinks that they may already have been victimized should contact their email provider right away.

The FTC has prepared a short video telling consumers what to do if they think they have become a victim of this scam. Youâ€™ll find it below.

byJim Malmberg
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 me on Twitter:

Follow ACCESS