Advice from Middle Aged Female Tech
Hollyecho Montgomery - 812-779-6088
Women's Computer Consulting
http://hollyecho.com

I have been in the industry with my own company since 1994. The entire time I have worked in this field there have been very few times any two techs ever agree completely. The advice I give here is based on my experiences, testing, and what I know works or to be true.

Today's Subject: Facebook scams and why users fall for them

This article is written by: Zeljka Zorz, An award winning editor – Very Informative.

The two main reasons why scammers are grateful for Facebook's existence are the fact that they can easily access a great number of people in a short period of time, and the fact that victims often end up "endorsing" the scams and by doing so add an aura of legitimacy to them.

It's easy to get lulled into a false sense of security, as Facebook often seems like a private and secure part of the Internet where one meets up with friends and family and mostly keeps tabs on their personal matters. But, it's not, and every user would do well to remember it.

Here is a list of the most popular scams lurking on Facebook, often repeated with small modifications, and obviously still successful.

Facebook account-themed scams

Facebook changes its look and functionalities often, but a lot of users dislike any kind of change. This normal human tendency is often misused by scammers who offer bogus Facebook Timeline deactivation options.

An even greater number of scams targets those who aren't satisfied with features offered by the social network and are tricked into believing that there are ways to add functionalities such as the ability to view who checks out their profile more often, view who has deleted or unfollowed them, to see how many hours they spent on Facebook, to post again their first post, to add a Dislike button, to change their Facebook color theme, and even to add a Facebook security app to guard their accounts or to try a Facebook 2013 Demo app.

Next we have the scams that profess that Facebook is giving out something for free: an official Facebook T-shirt or mug to celebrate the social network's birthday, the random $50,000 reward, free Facebook Credits, or even a free mobile recharge.

Lastly, there are scams that try to scare users into doing something because Facebook is closing all accounts, will close theirs because of overpopulation, will start charging users, or the Facebook Security Team will suspend their page.

It's also good to know that Facebook-themed scams - and especially phishing attempts and malware-infection attempts - can often come in the form of fake Facebook notification emails - password change notifications, account cancellation (or deactivation) warnings, offensive comment notices, friend requests, and so on.

Scams that offer free goods from third-parties

Many of these scams target users that want Apple devices such as iPads, iPad Minis and iPhones. There are also bogus $200 Ebay gift cards, $500 Target vouchers, airline tickets, Breaking Dawn Part 2 tickets, and more.

Scams that take advantage of news or fake news

It could be fake news about the death of a famous individual, real news about such a death, natural disasters, human tragedies, and anything else that has the potential of capturing the attention of millions of people around the world.

Scams that take advantage of the innate curiosity of people

There's a wide variety of amazing, funny, embarrassing videos and photos, often grabbing the victims' attention with messages that start with "OMG!!!", "WTF!!!" and "I can't believe that..." These appear on a daily basis and usually spread very fast on the social network.

What are the scammers after?

They aim to get some or all of these things:

- Email address and phone number for spamming purposes
- Personal information for identity theft purposes
- Facebook login credentials (username and password) in order to hijack the users' account and spread scams through it
- Users to inadvertently subscribe to pricy mobile services (by hiding the fact in very small print at the end of the page)
- Users to inadvertently allow continuous access to their account to malicious Facebook apps, along with the ability to post things on the users' Timeline in their name
- Users to complete online surveys so that the scammers can get paid for each one
- Users to "Like", "Share" or in any other way inadvertently or knowingly promote a wide array of scams and pages that are set up for the sole reason to spam their followers
- Users to download malware, adware or grayware disguised as YouTube plugins, video player updates, and similar legitimate software.

Why do these scams succeed over and over again?

There are many reasons:

- Users can't curb their curiosity
- Users - especially Internet novices - are not aware that such scams exist so they are easily tricked or scared into clicking offered links

- Users implicitly trust posts and links on Facebook because they originate from friends and family
- Users wrongly consider Facebook a safe place on the Internet.

Many users don't even bother to learn about these scams, and will fall for them over and over again because they either fail to realize they fell for them already, or that the fact that they did not get the free iPad, a new Facebook feature or saw the funny video is not because they failed to do what was asked of them or there was a glitch in the app or the Internet, but because these things weren't there to be had in the first place.

I am always about saving money and not spending it on things you don't need to

Remember ANY questions, email me at: **Montgomery@Hollyecho.com**. If possible, I will include the answer to your questions in my next article.