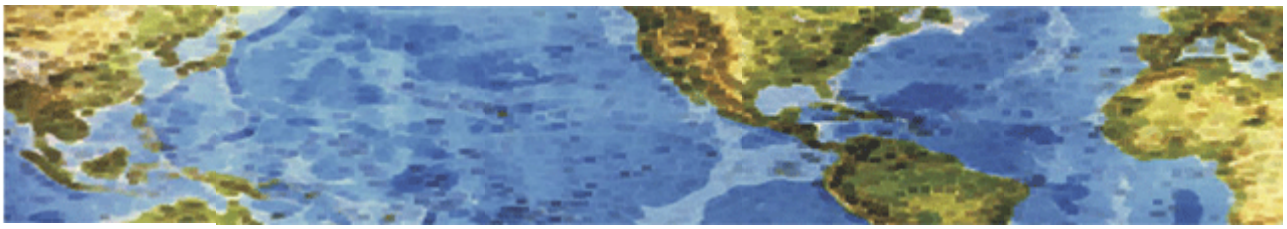
HALL ASSOCIATES



Risk-Based Decision Making Commentary
April 10 2013 Newsletter

Secure Your Facebook Timeline

The new Facebook Timeline is supposed to make your profile look newspaper like and let you look at your older information instantly. Looking at the security and privacy implications of any new Facebook (or any social media application/feature) is essential and a couple of actions are recommended.

This new feature lets your friends, and depending on your privacy settings, complete strangers view and navigate with ease a comprehensive history of your (or your kids or employees) life as posted on Facebook. While most of your existing privacy settings are maintained in Timeline, there are three actions that you may want to consider to make it more secure.

First, you can make all your past posts accessible to Friends only. When you first started using Facebook, you may have had more relaxed privacy settings than you do now. As a result, some of your older posts *(remember that everything you send/post is forever in this digital age)* may be more public than they should be. Timeline lets everyone navigate your older posts with ease. To cover this Facebook has a feature called "Limit the Audience for Past Posts". This will change past posts from whatever their current state is to "Friends Only". However, if friends are tagged in them, then friends of friends may still be able to see them. *And do you know who your friends have friended*?

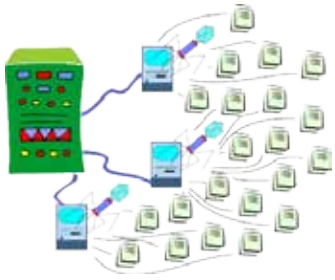
Second, set your default privacy setting for future Timeline posts. You should customize your default setting for all future posts in the privacy settings menu so only your friends can see them.

Third, consider enabling the Timeline Review and Tag Review feature. Since there are things that you would never want posted on your Facebook page, it is useful that you can review and decide if something will appear on your Timeline before it is published. With the Timeline Review and Tag feature, you can review and decide if you want a post to be published prior to it showing up on your timeline.

http://netsecurity.about.com/od/securityadvisorie1/a/How-To-Secure-Your-Facebook-Timeline.htm

The http://netsecurity.about.com/od/newsandeditorial1/u/Protect-Mobile-Devices-Smart-Phones-Ipad-Mp3-Players-Etc.htm website provides a lot of information about how to protect your social network accounts and mobile devices.

HALL ASSOCIATES



vSkimmer Botnet Targeting Payment Card Terminals Connected to Windows

McAfee has shared details of a new botnet circulating on criminal forums, mostly out of Russia, which targets payment card terminals connected to Windows systems. The botnet, named **vSkimmer**, has been around since February and appears to be an ongoing project for the person selling it.

vSkimmer seems to be the successor to Dexter. Dexter is the financial malware responsible for the loss of nearly 80,000 credit card records and the successful breach of payment card data at scores of Subway restaurants in 2012. vSkimmer has more functionality when compared to Dexter. In a forum post, vSkimmer is pitched as an advanced tool that will capture credit card data from systems running Windows that host payment processing software. vSkimmer is supposed to detect card readers and capture all of the track data collected, encrypt the data and ship it off to a control server for later retrieval. It uses a whitelisting routine to look for actionable processes, by checking each process run on the system that isn't on the ignore list and using pattern matching to extract the card's Track 2 data. Track 2 is where the card number, three-digit CVV code, and expiration date are stored on your card.

If present in the terminal software, vSkimmer says it will also ferret out any additional data, including names and PINs. This botnet is particularly interesting because it directly targets card-payment terminals running Windows. Like Dexter, vSkimmer is said to be completely undetectable on the compromised host.

http://www.securityweek.com/vskimmer-botnet-targeting-payment-card-terminals-connected-windows

Spear-Phishing Attack Targeting Android Devices

This is part of an emerging trend – phishing attacks using Trojans that can compromise not just mobile devices, but also the PCs and Macs that these devices connect to. This particular attack involved an APK – a program for the Android operating system that allows users to download G-mail attachments. This malware has the ability to secretly report back information about the user to a server and could harvest information such as contacts, call logs and SMS/text messages stored on your device. Having access to contacts is one of the things a scammer needs to make a spear phishing campaign successful. Scammers are increasingly gathering information about mobile and online users through groups they are affiliated with and social media channels (see the above Facebook note).

http://www.govinfosecurity.com/interviews/spear-phishing-goes-mobile-i-1877