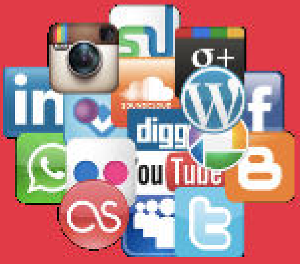

SOCIAL MEDIA SECURITY

facebook

Settings should never be weakened, only strengthened. The settings can be found at https://facebook.com/settings. You should first review “Privacy” to see who can view your profile, tag you in images and contact you. These settings, when strengthened, make it difficult for strangers to find lots of information about you. Facebook also allow you to check who has tagged you in what before they publish it on your “Timeline”. All posts and images will be stored and everything you post you should consider it as accessible online forever.

LinkedIn

As with Facebook, you should never weaken any default security and privacy settings on LinkedIn. Settings for your profile are found at https://www.linkedin.com/psettings/ and here you can choose who can see all of your connections. You can also pick who sees the “viewers also viewed” function and enable two step verification - which is a very good idea. Be careful what you share on LinkedIn - not all of the information there will help your job profile but will help attackers to profile you. If attackers can find out almost everything about you on LinkedIn, they can use this information for social engineering. Impersonating you can become easy and this is a large risk to your business. Think before you post.

twitter

Profiles on the micro-blogging site are automatically set to public. This means anyone with an account can view all of your tweets, people you follow and the people that follow you. This can build up a good profile of your interests, hobbies, thoughts and political views. As with LinkedIn this can be used to impersonate you or social engineer you. For example an attacker could use interests you’ve tweeted about in phishing emails or telephone scams. If your account is set to private in settings - found at https://twitter.com/settings/account - your tweets can only be seen by people approved by you. If you do require a public Twitter account, be very careful about what you post. It will be there forever. Twitter also supports two step verification via SMS, this could be a good additional security measure. If your location is on in your Tweets, they can be very accurately geolocated - so it is a good idea to turn this off.

www.sbrcentre.co.uk

Scottish Business Resilience Centre
Creating a secure Scotland for business to flourish in