

Social Networking is now one of the biggest activities online. Millions sign up to social media sites like Facebook and Twitter each year.

And according to Digital Buzz, Facebook is now used by 1 in 13 people around the globe, and the average user has 130 friends and that is set to grow.

However, this growth has brought with it a new set of threats which you need to protect yourself from.

Fortunately, sites like Facebook, Google+, Bebo and Twitter take privacy rules seriously and have poured lots resources into protecting you.

But they've failed many times too and have come under fire in the past for some of their lax rules which have opened many to harmful threats. And unfortunately their protection features won't shield you from some forms of phishing scams that are complex and hard to identify.

Threats found on social media sites

Threats in the social arena are many and varied and they continue to rise. Some are targeted at children and the vulnerable, and the criminals behind them are sophisticated and persistent.

And some threats are from cyber criminals looking to steal your identity.

1. Phishing

Most people are unfamiliar with the term phishing despite it being one of the biggest threats online.

It has been around for years and mostly occurs in email communications and if you check your inbox, you'll probably find an example in your spam or junk folder.

A common phishing scam is an email claiming to be from your bank and saying your details have been compromised and you need to update your account through a link in the email. This leads you to a fake website where your details will be stolen and your money too.

This is one example out of many phishing attacks and Facebook, which has hundreds of millions of users, is a paradise for cyber criminals.

By setting up fake accounts or using stolen ones, criminals can send out friend requests and use any info you share to steal your details. One common example is finding out when you're on holiday and helping themselves to your goods and property.

2. Cyber bullying and Harassment

Children are the most vulnerable to bullying and harassment and the dangers are potentially greater than other social networking threats.

Because of the non-confrontational nature of social media, people are bolder in saying things that they normally wouldn't in person. And because of this, it is easy to create anonymity and appear as what they are not.

Smartphones and mobile phones also compound bullying and harassment problems inherent in social media. And this can be done anywhere without parents' knowledge of what is taking place.

The first step is to educate your children on the dangers they will face as they use social sites. And secondly, you should use Parental Controls to restrict excessive usage of these sites and block all explicit content.

Kaspersky antivirus has the best parental controls which allow you to easily configure to your specific needs and set passwords.

The best antivirus software

Overall, Kaspersky is the best antivirus software program for social networking. It helps you defeat phishing scams so you don't fall into the traps that many fall into.

Hackers have created fake Facebook sites that look as real as the genuine site and they have used these to steal millions of Pounds and identities.

With Kaspersky, all scam sites will be blocked by the antiphishing feature.

[telefon dinleme](#)