How not to get hacked

Gone are the days when we could live in peace believing that as low-profile individuals, we were unlikely to draw the attention of hackers. Any information shared or stored online is now prized by cybercriminals, many of whom make big money targeting ordinary individuals.

Source: pixabay.com

“Sold to marketing companies or used to hold people ransom, personal data and browsing history are very valuable. We cannot afford to be careless about what information we share online or with whom,” says Thomas Vollrath, head of local hosting company 1-grid.com. The company specialises in helping small to medium sized businesses get online securely, without compromising their employee or customer data.

Individuals can take precautions to make themselves invisible online, Vollrath offers some useful tips:

Know who you share your data with – only give your personal information and banking details to secure sites that belong to trusted service providers. Check that there is a privacy policy in place that clearly states your data will not be shared with any third parties.

Avoid public Wifi – it is best not to enter any personal information online while connected to public Wifi networks, including those in coffee shops. Do your online banking at home or on a more secure network, like your phone's hotspot.

Enable two-step verification – this is important not just for banking apps, but also your email account. Valuable information about yourself and your work passes through your email account – make sure that it is difficult for hackers to crack.

Mind the apps – a single app with too many permissions can seriously compromise your data. Think carefully about what information you are willing to share with each app you install.

Store and dispose of info securely – have strong passwords on all devices that have access to your personal information and accounts. Wipe all data off your laptop and cell phone before giving them away or selling them.

Keep an eye out for impersonators – phishing schemes impersonate people or companies that you know in order to trick you into sending them valuable information. Always check sender details carefully and never enter information into links you receive via email. Rather Google the company, go to their official site and sign in there – or call customer support to check that the email is legitimate.

Secure your domain – if you own a domain yourself or for your business, your name, email address, telephone number and physical address is published online in the WhoIs database. You can make this listing secure and private by purchasing security for your domains.

"The internet is an integral part of everything we do – our work, banking, administration and social lives depend on it. Being secure does not require abandoning the online world entirely, but everybody needs to take precautions," says Vollrath.