BIZCOMMUNITY

Be aware of domain hijacking

Domain names can be stolen, held hostage and used to wreak havoc for a business website owner. Domain hijacking, as it is called, entails cyber criminals unlawfully gaining access to a website's unique domain in order to impersonate the business for other illegal activities such as phishing and harvesting customer information.

Thomas Vollrath, head of local hosting company, 1-grid

With the passing of the Protection of Personal Information Act (POPI), businesses can face lawsuits if they do not take reasonable steps to protect customer data stored on their domain from this form of cyber attack.

“A domain should always be renewed on time. If a domain expires or enters a redemption period, it is often very difficult and expensive to redeem. If the domain is eventually deleted from the registry, after the redemption period, it becomes available again. Anyone can legally claim it,” says Thomas Vollrath, head of local hosting company, 1-grid.

A hijacked domain is a worst-case scenario for a business with a website. Possible fallouts include lost revenue, reputation damage and financial penalties for failing to protect customer data. Not to mention the loss of the URL customers type in to find your business. “Think of it as brandjacking,” says Vollrath.

Take action

Here are tips on what you can do to prevent your domain from getting hijacked:

- **Practice strict online security** – strong passwords, two-factor authentication and knowledge of how to spot a phishing scam are crucial. Most hijackers get control of a domain by getting hold of the personal and login details of the individual in whose name it is registered.

- **Enable WHOIS protection** - WHOIS protection hides information like your physical address, telephone number and email address from people looking into your website's domain. Cybercriminals have been known to use this information in impersonating domain owners.

- **Choose a good domain registrar** – look for things like full DNS control, automatic domain locking and good technical support in the company you choose to register your domain through. These features ensure that domain registrations cannot be changed without authorisation.

- **Get a watchdog for your website** – one of the first things cybercriminals will do is transfer your domain to another registrar, making it very difficult to get it back. Strong, 24-hour website security ensures that suspicious activities are picked up and flagged immediately, day or night so that actions can be taken to stop the transfer of your domain before it's too late.

"Aside from the loss of business and brand damage incurred by a domain hijacking, attackers often go on to stage elaborate phishing campaigns and other scams targeting your business and its customers," says Vollrath. Some hold domains ransom, demanding money for their return - or, depending on the value of the domain, sell it for a lucrative sum.

With a focus on SMBs in South Africa, there are web security packages, domain, web and email hosting, a website building tool, SSL certificates, website design and online marketing expertise available. "SMBs are vital to the growth of our economy – but they need real and affordable online expertise, support and tools to keep their data secure and their sales growing," says Vollrath.