PROPERTY SCAMS – BEWARE (CYBER) WOLVES IN SHEEP’S CLOTHING!

“Beware the wolf in sheep’s clothing” (Aesop’s Fables)

Cybercrime levels are surging, and it didn’t take the scammers long to figure out that when you buy and sell property you become a prime target because of course –

Property transactions provide rich pickings, often very rich pickings.

Electronic communication between attorneys and clients, which is all-pervasive these days, creates a fertile ground for interception and deception.

Consider this nightmare scenario

You’ve sold your property for R5m, transfer to the buyer has been registered but the money doesn’t show up in your bank account (let’s call it “account A”). You phone your conveyancer only to be told “but we did pay you, we followed your instruction to pay into account B.” Of course account B was set up by a scamster and your R5m is long gone. What happened?

How the scams work

Cyber criminals are resourceful and creative so this is by no means an exhaustive list of your risk areas, but currently the two main ones seem to be –

Your attorney’s payments to you: As a seller, when you give the transfer instruction to your attorney you will nominate a bank account – account A in this example - to receive the sale proceeds. Before transfer however (often at the very last minute) the firm receives a genuine-looking email “from you” changing your banking details to “my new account, account B”. Your emails to and from your attorney have been intercepted, and your details cleverly spoofed. Your money is gone – forever.

Your payments to the attorney: The main risk here is to the buyer paying the whole or a large portion of the purchase price to the transferring attorney. Of course transfer duty and other costs of transfer can also add up to a tidy sum, whilst as a seller you will be paying for things like bond cancellation costs, rates, agent’s commission and so on.

The scam here is that once again emails are intercepted, and this time you receive an authentic-looking but entirely fraudulent email asking you to pay into “account C”. The email appears to come from the conveyancing firm but of course it is again a clever (often very sophisticated) spoof, this time of the firm’s branding, details and email address.

The false account details might be in the email itself or in a falsified attachment – nothing is safe. The email may be in the form of a “we’ve changed our banking details” notification, or the criminal may work on the basis that you just won’t notice the change. And of course account C isn’t the conveyancer’s trust account at all, and the minute you make a payment into it your money is - once again - gone forever.

How can I protect myself?

The problem normally starts with criminal interception of emails or hacking of online data and what follows is a classic case of a “wolf in sheep’s clothing” deception.

Here’s your essential checklist to minimise the risk -

Keep all your anti-virus, anti-malware and other security software updated, learn all about protecting yourself from malware/spyware/phishing attacks (your bank will have tips for you – see e.g. Nedbank’s “Fraud Awareness” page here), and generally treat all electronic communications with caution – even those appearing to come from a trusted source like your attorney.

Read “Is That Sender For Real? Three Ways to Verify the Identity of An Email” on FRSecure’s blog. All the tips given there are important, but at the very least use the methods given to find out where the email really comes from. Then check back to see that it matches in every detail the email address you were given at the start of the transfer process.

Be suspicious if anything in the email just feels “not-quite-right” – perhaps only a cell phone number is given, or a free generic email address (like Gmail) is used, or the wording is somehow “off”. If the email makes you even the slightest bit uneasy, err on the side of caution and investigate further.

Most importantly, never accept notification of any change in your attorney’s banking details without visiting or phoning your attorney to check all is in order (don’t of course use the phone number given in the suspicious email!).

A final thought – are you the weakest link?

As a client it’s no use relying on your attorneys to have all the latest security systems and procedures in place. Think of how banks enforce stringent security protocols and protections, yet still their customers are regularly scammed. If your own computer, network or actions are the weakest link in the chain, then that’s what the criminals will exploit!

Follow the above tips to protect yourself and if you ever have even the slightest doubt about anything, take no chances and contact your attorney to check!