BLOOM MICROTECH
Discover Real Service

FROM BEHIND THE SERVICE COUNTER

We've noticed a sharp increase in clients getting compromised or scammed through the internet and with a bit of care it can be easily avoided. Here's a few tips to follow to keep yourself out of trouble;

Tip #1. Always be cynical. Is the offer too good to be true? That's a warning! Is the offer sent to "My friend" or "Dearest" or "Hey buddy"? If the salutation is impersonal, that's a warning!

Tip #2. Check properties on incoming emails. Unfortunately this works best in Outlook. If an email is coming from an unknown source, right-click on the email and look at its properties. This will reveal the part that shows who the true source of the email is. Quite often "John Doe" is suddenly revealed as "Bounce_back_coupon" suggesting that you should just delete the email. **Always refer to Tip #1.**

Tip #3. If your antivirus program says something is bad, don't still check it out "just in case". Some products like ESET's NOD32 (our favourite) will move an infected email to an "infected" folder. If it's infected, don't activate it by even looking at it. Trust us, there's nothing there for you but trouble. Click DELETE. **Always refer to Tip #1.**

Tip #4. Just because you find a link, you can't believe it is what you see. Many hidden links are coded into what look like regular links. You think you're clicking on some banking site because they've asked you to update your info when in fact you're about to give the bad guys all your personal data.

We have also seen these come from "Revenue Canara" (note the spelling mistake) with the offer of a tax refund. You'd be surprised how often these ploys succeed. We've come across a case where this tax refund scam did work and we had to advise the client to immediately change all their bank and email passwords.

The best way to defend yourself is hover your mouse over the link or right-click and review its properties to see what the real destination is. And refer to Tip #1, something purporting to be from the Royal Bank that actually points to www.royal-bank.asia.com is probably NOT a good bet to pursue. **Always refer to Tip #1.**

Tip #5. Check for obvious spelling mistakes. Thankfully many of these web bandits can't spell worth a damn. Anything with grammatical or spelling errors is probably bogus. **Always refer to Tip #1.**

Tip #6. Never click a link or open a document just because an email tells you to. Emails can arrive from a "friend" with just a link to click or a document with a message to open the document for further info... It must be okay because it came from a friend? No! STOP! Don't do it! If you think it is real, call them or email them and ask them for confirmation first. More than likely they are infected and their virus is just trying to spread the joy to you. **Always refer to Tip #1.**

Tip #7. Check to see who the email was sent to. In the "TO:" line, are you one of a bunch of other names you don't recognize? This again is typical of a friend's system that is infected and is just trying to share. **Always refer to Tip #1.**

Tip #8. Just because an email appears to come from someone you know, it in fact may not. Hotmail and Roger's email accounts have proven to be easy pickings for password hackers. If your password is not complex (i.e. - "Home123" or "paSSword") hackers can compromise your account and start pestering your contact list friends with spam, spam that you get blamed for! **Always refer to Tip #1.**

Guard yourself. Strengthen your password with a capital letter, a few numbers and some specialty characters like #, $ or !. …and do it NOW!

You have to exercise a healthy amount of cynicism when looking at the web. Bad people abound and are waiting around every corner. Stay skeptical, stay safe and always refer to Tip #1.

Harley Bloom
Bloom MicroTech