TIPS IN PREVENTING IDENTITY THEFT

Identity theft and credit card theft is fast becoming a choice method of white collar criminals in the theft of money and property.

Online identity and credit card theft usually occurs when the unsuspecting person gives his or her personal information by email or through online web forms.

This is normally done through a fraudulent website designed to appear like a genuine institution.

Virtually anyone with email or access to the internet is exposed to this crime, especially if such person has online financial transactions eg online banking.

An example of such a fraudulent attempt is found in the following email and corresponding website.

From:	**"Chase Manhattan Bank Security Department" <account@chase.com>** Add to Address Book Add Mobile Alert
To:	**dsjsws@yahoo.com, ncrwcc@yahoo.com, kevinchao@yahoo.com**
Subject:	**WARNING: CONFIRM YOUR ONLINE BANKING RECORDS**
Date:	**Wed, 14 Sep 2005 11:56:54 -0300**

In attention of JPMorgan Chase & Co. customers,

As the Internet and information technology enable us to expand our services, we are committed to maintaining the trust customers have placed in us for protecting the privacy and security of information we have about you. In order to protect your information against unauthorized access, identity theft and account fraud we earnestly ask you to update your profile.

To get started, please click the link below:

https://chaseonline.chase.com/accountservices.jsp

Thanks for your patience as we work together to protect your account.

Regards,

Customer Support Center.

This kindof fraud is fairly easy to prevent if you remember:

a) That financial institutions shall never request you to confirm your personal information by email or on the internet;
b) To always seek oral confirmation from the financial institution on the information sought, through a landline that you know to be genuine;
c) To always look out for the prefix: ***https*** before the name of the website, as well as a padlock at the bottom of the computer screen as indicators of a secure website

With regard to identity fraud affecting financial institutions, these institutions need to satisfy themselves as to the identity of the person opening accounts, giving them instructions and authorizing the release of funds.

In Kenya's financial circles these days, it is common to find persons opening bank accounts with identity cards that do not belong to them, or banks cashing cheques to the wrong persons.

A few pointers go along way in preventing the occurrence of this type of white collar crime. These are :

(i) that financial institutions should insist on as much identification documentation as possible, over and above a mere identity card, for instance, copies of water bills, electricity bills, letters of confirmation from other banks where the prospective customer has an account etc
(ii) that Cheques should NEVER be sent by post;
(iii) that financial institutions should always be very cautious in cashing cheques which are dated BEFORE the date that an account is opened with the institution. They should always contact the drawer of the cheque to confirm their instructions. Too many fraudsters are stealing company cheques, altering them, opening accounts with a similar sounding name as the payee, and cashing them.

Article by researchers at the National Centre for Research on White Collar Crime, NCRWCC, Nairobi

Email: ncrwcc@gmail.com