

IDENTITY FRAUD: PHISHING SCAMS

Courtesy of the US Federal Trade Commission

available on line at

www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm

Phishing it is one of the newest forms of identity fraud and it involves Internet fraudsters who send spam or pop-up messages to lure confidential information (e.g. credit card numbers, bank account information, passwords, or other personal information) from unsuspecting victims.

Phishers send an email or pop-up message that claims to be from a business or organisation that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your account information. Some phishing emails threaten a dire consequence if you don’t respond. The messages direct you to a website that looks just like a legitimate organization’s site. But it isn’t. It’s a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

If in doubt:

- If you are in any doubt about the source of an email or request for such information claiming to come from us or of the validity of a website, contact us on 0860 30 92 50 or 0860 11 99 25 or e-mail us at callcentre@mercantile.co.za.
- You may also want to open a new Internet browser session and type in Mercantile Bank’s correct Web address yourself. Our address is www.mercantile.co.za. In any case, don’t cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.

Please remember:

Mercantile Bank will never ask for your username or password via email.

How not to get hooked by a phishing scam:

- Under no circumstances enter any of your personal or account details.
- If you get an email or pop-up message that asks for personal or financial information, do not reply. And don’t click on the link in the message, either. Legitimate companies don’t ask for this information via email.
- Use anti-virus software and a firewall, and keep them up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.
- Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognises current viruses as well as older

ones; that can effectively reverse the damage; and that updates automatically. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.