



# GiRO NEWS

NEWSLETTER - JULY 2015

In this first newsletter we will deal with the inevitable topic of **banking information security**.

## WELCOME TO GiRONEWS

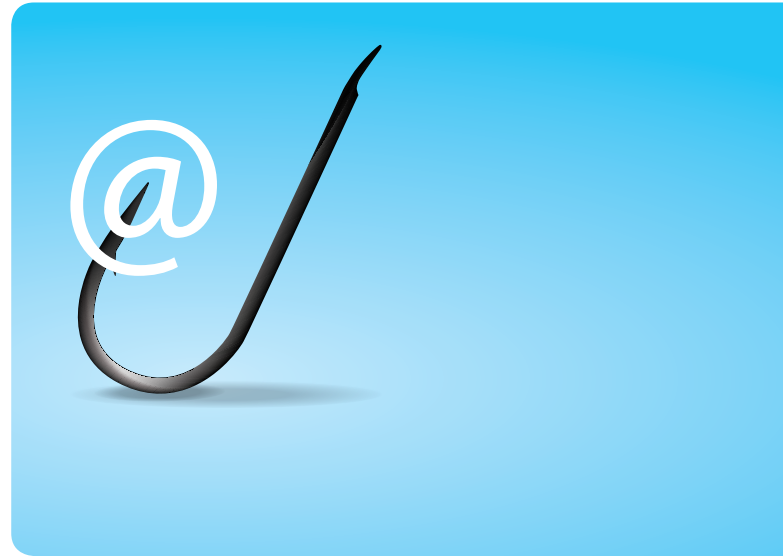
At Girobank, we like to keep our clients up to date on new products and services, market developments and other relevant issues.

As of today, there will be a regular Girobank newsletter to keep you posted! This newsletter will not only be available in our branches, but also on our website, [www.girobank.cw](http://www.girobank.cw), and on our Facebook page. If you haven't 'liked' the Girobank Facebook page yet, please do so to stay updated.

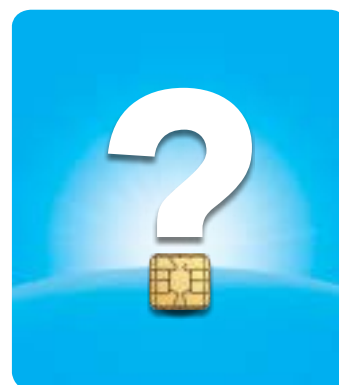
## NEW activate it!



In a couple of weeks we will launch another innovative feature of our online banking service Gironet called Activate It. No need to call the bank anymore when you are traveling or are planning to make a large purchase. You will be able to easily activate your profile and status through Gironet. Easy, convenient and fast. More information about the service roll out will be provided soon.



## GIROBANK CHIP CARD is coming soon!



In a few months, we will launch the new Girobank Chip Card. Our cards will use the latest technology called EMV, which stands for Europay, MasterCard and Visa. This chip technology makes cards safer and harder to skim when used at ATMs and Point of Sale Terminals (POS) that use this technology.

We are currently upgrading our cards, ATMs, and Point of Sale terminals with the EMV chip technology. Unfortunately, you could experience some downtime of our ATMs, while we are in the process of upgrading them. We are undoubtedly doing our utmost to get the job done as swiftly as possible and apologize in advance for any inconvenience. Soon, you will receive more information as to when your new chip card will be ready for you.



## WATCH OUT FOR FRAUDULENT E-MAILS & SKIMMING!

### Fraudulent e-mails

It has come to our attention that there are several fraudulent "Phishing" e-mails circulating that claim to be from local banks, among which Girobank N.V. In these so called "Phishing" e-mails, clients are requested to click on links that direct them to a forged website to provide their username, password, the access card grid numbers or other sensitive information. With this information criminals could potentially perform unauthorized transactions from your account, misuse your identity or perform other malicious activities.

It is important for you as a client of Girobank N.V. to know that Girobank N.V. will never present you with this kind of e-mails. We will moreover never ask you to disclose, update or validate your account information, such as but not limited to, your username, password, pin, access card grid numbers, credit card number or debit card number via e-mail. Account information is strictly personal and should never be shared with any company through e-mails or any other means (e.g. phone, personal conversations, etc.). Never click on any link or open attachments within these e-mails or engage in any other type of unsolicited (online) request related to your account information.

### Skimming

You have probably read it in the newspapers or heard it on the radio or perhaps you even know someone who has been a victim of it: Skimming. Unfortunately there have been many of these cases of fraud in Curaçao lately. Skimming is extremely harmful as it is mostly performed in a way that is hard to detect.

Debit cards or credit cards are copied while they are used in a legitimate transaction by a cardholder, for instance behind a store counter, or by putting a special device on an ATM machine. When the card is copied, the criminals involved need to get hold of the security code (PIN). They will usually obtain this simply by looking over someone's shoulder when he or she is making a payment or by implementing other more sophisticated techniques such as the use of cameras. With the copied card and the PIN, the criminals can make purchases in stores or withdraw cash from an ATM; this process is called harvesting. At Girobank, we are committed to do everything within our reach to prevent skimming and harvesting from happening.

Skimming can cause a lot of damage in a small period of time. Therefore, it is important to be careful while using your cards. Please find some tips to avoid skimming and its consequences.

## WHAT CAN YOU DO TO PREVENT SKIMMING?

- 1 Never let anyone use your debit or credit card;
- 2 Always make sure other people are not able to see your PIN when using your card, for instance by shielding it with your hand;
- 3 Do not use ATM machines if you notice something's not right;
- 4 Change your passwords periodically (for example: every two months) and immediately if you suspect it might be compromised.

## WHAT CAN YOU DO TO PREVENT PHISHING?

- 1 Do not disclose personal data, account information, passwords, access card grid numbers, pin, credit card numbers and/or account numbers via unsolicited e-mail correspondence or websites, even if such an e-mail claims to be from a company (including banks);
- 2 Do not update your personal information or change your password on any website other than your secure online banking system after logging in; To be sure that you are on the secure website of Girobank N.V. enter the URL manually and check if the URL (the bar all the way up at the left side of your login screen) has a combination \* of the following characteristics prior to starting the login process:
  - a. The color of the bar (or text in it) is green;
  - b. The name of the site starts with: "https://personal.gironet.com/";
  - c. The bar has a closed lock (🔒) and the name: Girobank N.V. [CW].
- 3 Change your passwords periodically (for example: every two months) and immediately if you suspect it might be compromised;
- 4 Always log out when you finish using your e-mail and/or finish using your online banking;
- 5 Only access online banking from a secure system. This includes:
  - a. Install only legal and proven software;
  - b. Ensure that you are using the latest version of your applications and operating system;
  - c. Install and frequently update an (proven) anti-virus product which includes anti-spyware capabilities;
  - d. Ensure that a firewall is installed and active.
- 6 Use a secure (WIFI) network when doing online banking. Check your bank account on a regular basis to identify any fraudulent transactions;
- 7 Take immediate action if you have the feeling - or have actually notice - that someone has made transactions on your account without your consent. You can contact us daily 24 hours a day at +5999 433 9130 or send an e-mail to [info@gironet.com](mailto:info@gironet.com), whenever you notice anything suspicious;

*\* May differ from browser to browser.*

**Do not request a debit card for your savings accounts. The balance on savings accounts is generally higher than on current accounts. By accessing funds available on your savings accounts with a debit card, you may be exposing a higher amount in case of Skimming. Transfer funds between your accounts using Mobile Banking instead.**



# Girobank Alert Notifications,



## KNOW WHERE YOU STAND, AT ALL TIMES!

We strongly believe it's a bank's #1 priority to make life easier for its customers. We walk the talk and proactively provide you with useful information and anticipate on your changing needs and circumstances.

Our SMS and e-mail alert notifications provide you with instant update on your mobile phone with every transaction on your account. You will no longer need to anxiously anticipate when your salary or that important fund is deposited. You will receive an alert within seconds after the deposit is made. Need to be more in control of your personal finance?

The alert system can also automatically warn you if your balance reaches a certain level that you have indicated.

You can also receive SMS and e-mail alerts on any

transaction with your credit card. You will also see the remaining balance after every purchase in your e-mail alert. We do the math while you are shopping so you won't be unpleasantly surprised with a bounced credit card during your shopping spree.

We also use SMS and e-mail alerts to inform you about important matters. Please let us know if you have any questions about our alerts. You can always call us at +5999 433 9130 or send an e-mail to [info@gironet.com](mailto:info@gironet.com). If you are not receiving SMS alerts but would like to, please update your phone number on Gironet, at a branch near you or call one of our customer service representatives.

*With our alert notifications, you always know where you stand.*

NEW!

## e STATEMENTS

Help us protect the environment.

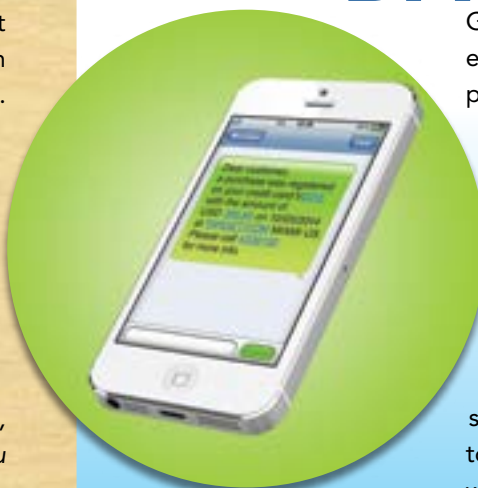
We have recently introduced e-statement, to enable you to receive your statements in an environment friendly way. E-statements are free of charge and are always within your reach on Gironet (Online Banking). E-statements are available faster than the old fashioned paper statement. So you do not need to wait on your statements anymore.



Please note that we will start charging for regular paper statements soon. Thus if you do not have an online banking account as yet, don't wait any longer. Visit your favorite branch today and apply for Gironet and e-statements.

*If you have Gironet already just login and follow the steps to apply for e statements. For more information call us on +5999 433 9130*

## mobile BANKING



Girobank Mobile Banking enables you to use your mobile phone to check your balance, recharge your phone, request a mini statement or make transfer between your accounts and receive transaction alerts anytime anywhere. All these transactions are processed real time, thus within seconds. For instruction how to use mobile banking visit our website: [www.girobank.cw](http://www.girobank.cw).

## contact INFO



We are frequently conducting research to remain 100% informed about the preferences, wishes, complaints and questions of our clients.

We also try to keep you posted on new developments, campaigns and other services. We use our website, SMS and e-mail notifications or Facebook page to keep you informed. In order to reach you we need to receive your current contact information. So if you have moved recently or changed your phone number or e-mail address, please let us know. Pay us a visit at the branch most convenient to you and please update your contact information. *Thanks in advance!*