Do you have the skills and did you discover any vulnerabilities in our systems? If so, help us by reporting these vulnerabilities. So that we can improve the safety and reliability of our systems together.

ING Direct and safety

As ING Direct we consider the safety of internet banking and the continuity of our online services as one of our top priorities. Every day and night, our specialists work on optimizing our systems and processes. Despite the effort we put into the security of our systems, vulnerabilities in our systems might still be present.

What to report?

Vulnerabilities with regard to the safety of ING's services offered through the internet. In case you have discovered a vulnerability in our system, please report this as quickly as possible. Examples of vulnerabilities could be:

- Remote code execution
- Cross scripting (XSS) vulnerabilities
- SQL injection vulnerabilities
- Cross-Site Request Forgery (CSRF)
- Encryption vulnerabilities
- Authentication bypass, unauthorised data access

Excluded from reporting

- All reported vulnerabilities without a properly described evidence report of proof of possible exploitation.
- Vulnerabilities found on sites of organisations that are no longer part of ING (former business units).
- Our policies on presence or absence of SPF/DKIM/DMARC records.
- Cross Site Request Forgery (CSRF) vulnerabilities on static pages (only on pages behind logon).
- Redirection from HTTP to HTTPS.
- HTML does not specify charset.
- HTML uses unrecognised charset.
- Cookie without HttpOnly flag set.
- Absence of using HTTP Strict Transport Security (HSTS).
- Clickjacking or the non-existence of X-Frame-Options on non-logon pages.
- Cacheable HTTPS response pages on sites that do not provide money transfer capabilities.
- User enumeration on sites that do not provide money transfer capabilities.
- Server or third party application version revealed and possible outdated without Proof of Concept on the exploitation of it.
- Reports of insecure SSL/TLS ciphers and other misconfigurations.
- Generic vulnerabilities related to software or protocols not under control of ING.
- Distributed Denial of Service Attacks.

- Spam or Social Engineering techniques.
- Reports of regular scans like Port scanners.

What is responsible-disclosure@ingdirect.es not used for?

- Reporting complaints about ING's services or products
- Questions and complaints about the availability of ING websites, mobile banking or internet banking
- Reporting monetary issues (e.g. ATM's and pin devices)
- Reporting Fraud or the presumption of Fraud
- Reporting fake e-mails or phishing e-mails
- Reporting malware or virus issues

How can a vulnerability be reported?

A vulnerability can be reported by e-mail; responsible-disclosure@ingdirect.es. A prerequisite for sending an e-mail to the above mentioned e-mail address is that you utilize the public PGP key (zip). Please ensure that your e-mail is written in a clear and succinctly way. Particularly include the following in your e-mail:

- The **steps** you undertook
- The entire **URL**
- **Objects** (as filters or entry fields) possibly involved
- **Screen prints** are welcome

Our specialists will read your report and start working on it right away. Did you find a vulnerability in one of our IT-systems. Please contact us directly and do not postpone.

Despite many of you used to send a video in which the vulnerability PoC is reproduced, we ask you to avoid this method as a way of reporting. This technique slows down the management of a possible impact, both at the origin (caused by spending time in the preparation and publication of the video) and at the destination (due the data extraction).

Am I eligible for a reward after my finding?

ING highly appreciates your effort by assisting us in optimizing our systems and processes. In case your reported vulnerabilities have been solved or led to a change in our services, you will be eligible for a reward. The amount of the reward depends on the severity of the vulnerability reported, the type of website (static information sites versus online banking sites) concerned and the quality of the report we receive.
If the report is of great value for the continuity and reliability of the bank, the reward will be considerably higher.

Can I report a vulnerability anonymously?

Sure, you do not have to provide your name and contact details in case you want to report a vulnerability. However, you should take into account that we are unable to discuss the next steps with you. For instance, we cannot inform you about what we will do with your discovered

vulnerability, neither we can collaborate further, nor we can provide you with the appropriate credits or reward in return for your finding.

Your privacy

Your personal information is only used to approach you and undertake actions with regard to your reported vulnerability. We will not distribute your personal information to third parties without your permission. Unless, the law requires us to provide your personal information or when an external organization takes over the investigation of your reported vulnerability. In this case we will ensure that the applicable authority will treat your personal information confidentially. We will remain responsible for your personal information.

What will we do with your finding?

A team of security experts will investigate your finding. Within two working days you will be receiving an e-mail with a first reply. Note: revealing your finding to the public is not allowed, instead talk to our experts and give them time to assess and solve the problem. Accordingly, we will provide you with feedback with regard to your finding. We will explain to you whether we will solve the problem, how we will solve it and when.

Rules

By investigating our IT systems, it might be that you act prosecutable. In case you act with good faith, act in accordance to the mentioned rules of the ING, there will not be any inducement to report your action. Therefore, follow the rules of the responsible disclosure.

- Ensure that during your and our investigation of your reported vulnerably, you do not apply any damage.
- Do not utilize social engineering in order to gain access to our IT-systems.
- Never can your investigation disrupt our (online) services
- Never can your investigation lead to the publicity of bank or customer data.
- Do not put a backdoor in the system. Neither with the purpose to show the vulnerability. Putting a backdoor will bring damage to the safety of the system even more.
- Do not apply any changes or delete data in the system. In case your finding requires a copy of the data from the system, do not copy more than your investigation requires. If one record is sufficient, do not copy more.
- Do not make any changes in the system.
- Do not attempt to penetrate the system more than required. In case you successfully penetrated the system, do not share gained access with others.
- Do not utilize any brute force-technics (e.g. repeatedly entering passwords) in order to gain access to the system.
- Don't use techniques that can influence the availability of our (online) services.
- If your reported vulnerabilities have been solved or have resulted in a change in our services, you will be eligible for a reward.
- Vulnerabilities detected by ING employees or former employees of ING are excluded from any rewards.

- Multiple reports for the same vulnerability type with minor differences will be treated as one report (only one submission will be rewarded)

Remaining conditions

- We can only process reported vulnerabilities that are reported in Spanish or English.
- In case you are eligible for a reward, we require your personal information.
- In case your reported vulnerability is reported by others as well, the reward will be granted to the first reporter.

Responsible Disclosure regulation

To check more information regarding IT Security matters, the 'Instituto Nacional de Seguridad' (INCIBE) in Spain has created numerous of technical guides that can be visited at https://www.incibe.es

Aberrant international regulation

We advise you to take into account that regulations with regard to the Responsible Disclosure differ per country. In case you are living abroad and have found vulnerabilities in one of our ING-pages, please realize that the Responsible Disclosure policy is not applicable in every country. This implies that despite you acted in accordance to ING's Responsible Disclosure policy, it might still be that you will be prosecuted by justice, despite we do not report the vulnerability to justice.