











****

Table of contents

[**1. Executive summary**](#_1oaqlpuieb27) **1**

[1.1 Introduction](#_th769one907z) 1

[1.2 Methodology](#_s2mdhvbzgs67) 1

[1.3 Results](#_ozr25zcryc9w) 2

[1.4 Recommendations](#_2rz50z3caa6a) 2

[**2. Scope**](#_4jnsfpl3vf4x) **3**

[2.1 Goal](#_65wy8j2ticq) 3

[2.2 Campaign](#_j38c5ywz6mk8) 3

[2.3 Data Collection](#_oqobt5ftwou4) 3

[2.4 Campaign Limitations](#_fzb6igwnrigd) 4

[2.5 Data Processing](#_llj1el9uoboa) 4

[**3. Methodology**](#_1uc7v5o8r1r4) **4**

[3.1 GoPhish](#_s51k3h61m04f) 5

[3.2 Domain](#_wp0e7ip7flmo) 5

[3.3 SSL](#_il4ot3c789wt) 5

[3.4 Website](#_crr8wwfldjgg) 5

[3.5 Six principles of influence](#_8rwzrjgxm1z8) 6

[**4. Campaign**](#_5p1fts7wf8md) **7**

[4.1 Email](#_5ef2ivjn9d7l) 7

[4.2 Website](#_v3n1p7929vl) 7

[4.3 Account Registration](#_w8bivo1rp0l2) 8

[4.4 Identifiable markers](#_8vcmldvujrl0) 8

[4.5 Informing victims](#_ht6lzkoh6ope) 9

[**5. Results**](#_cwd0ejn9bv9q) **10**

[5.1 Campaign Results](#_kow4x18oah0) 10

[**6. Recommendations**](#_ykghx1p7lguv) **12**

[**7. Conclusion**](#_mckugmg802y4) **13**

[**8. Document information overview**](#_yjvbp4y3cmtx) **14**

[Revision history](#_a7kqar25a6s7) 14

[**9. References**](#_z07981onbgum) **15**

#

# 1. Executive summary

## 1.1 Introduction

More and more companies and businesses are developing an online presence, but just like every other thing, everything comes with a price. This price being the security of the data which is put online and malicious users being able to access and steal that data. The word Phishing is known in this day and age, especially among the youngsters of this generation. However, how aware and critical are students of falling victim to such attacks? This still remains a mystery, so an analysis has been performed on the students of two bachelor programmes, in the effort to be able to get a better understanding of the following question:

*How aware are Logistic management and automotive students of Phishing mails and their downfalls?*

## 1.2 Methodology

In order to have this research question answered, an extensive research on the two bachelor studies was performed to get a better understanding of the students, their likings and what they find interesting. This was done through the Hogeschool Rotterdam website, which contained various documents about the course. After completing this research and a better understanding of our target audience was obtained, a Phishing campaign was put together in collaboration with Hogeschool Rotterdam's CERT team and Alex.

This campaign would entice the students to fall for a phishing attack on a fake webshop with interesting, cheap and time limited deals. This was to determine how vulnerable the target audience is to filling their personal data on a webshop with red flags. The deals were made time limited to ensure a sense of urgency was created to tap into their emotional decision making process, which ensured they fell for the attack.

Before being able to start the campaign, 2 green lights sessions had to be passed. These green lights were basically a confirmation for fulfilling all the criteria that had to be met before starting the campaign. The first session was to ensure that a proper plan was created, and the second session was to ensure that the execution of the plan was done correctly and to make sure nothing was missing. After passing both green light sessions the email list of the target audience was given by Alex. After this all that had to be done was to email the students with a convincing email to go on register on the website to be able to buy the deals. This was all done through GoPish which will be explained further in the research chapters.

After leaving the webshop open for a few days, a survey was conducted on the victims to find out what they thought about the campaign and if any snitching took place, which could help in understanding if anything could be done better in the future.

## 1.3 Results

Shortly after starting the campaign, the results came in. On the first day, several students submitted data through our registration form on the website. Though after that day off launch the results were meager. Reducing the number to +-2 data submissions a day. It might be possible that students warned each other about the email sent by us, resulting in less students falling for this. More about the campaign and a more in-depth look into the results will be discussed later in this report.

## 1.4 Recommendations

Every student falling for a phishing email is a student too much. It is important that students are more up-to-date with safety measures and are aware of potential dangers in the growing world of the internet. That's why it is recommended to give every student more information about the dangers of phishing and give them useful tips on how to avoid such scams. This can be done by giving short lectures to every student in the target audience, as Hogeschool Rotterdam currently does not provide that information.

# 2. Scope

The scope explains the goals needed to be achieved and what the restrictions are for this specific research, meaning the data which will not be collected and the reasons why. It also provides the research tools which will be used, how the collected data will be processed and then used to document the findings.

## 2.1 Goal

The goal of this phishing campaign is to find out how susceptible the students of the Hogeschool Rotterdam are to phishing. Our target audience are 239 students consisting of 3rd year automotive and 4th year logistics management students of the Hogeschool Rotterdam.

## 2.2 Campaign

The phishing campaign will consist of a single email and two landing pages. The email will be sent to the target audience convincing them to visit the website. Clicking on the link will redirect the student to the first landing page. The first landing page is the phishing page, this page is to convince the students to create an account. When the student has successfully created an account, it will redirect to the second landing page explaining the phishing campaign.

## 2.3 Data Collection

During this phishing campaign, data will be collected about the target audience. This data will consist of first name, last name, school email address and school name. The collection of this data will be done using GoPish, seeing that this framework provides tools and analytics for data collection. The plan is also to survey the victims to gain feedback on the campaign to form better conclusions.

##

## 2.4 Campaign Limitations

The phishing campaign has limitations set by the CERT team to prevent the target audience from losing their trust in the Hogeschool Rotterdam.

The first restriction is that the campaign cannot impersonate the Hogeschool Rotterdam or any affiliated organization. This means that creating a fake website or email that gives students the impression that it was sent by the Hogeschool Rotterdam or any affiliation is not allowed.

The campaign cannot contain a free-give-away or prizes-to-be-won campaign. These types of campaigns are too easy to create and don’t ask for any creativity.

No harmful data should be saved as part of this awareness test. This means that saving passwords, addresses or any other sensitive information of the sort is strictly prohibited as this information could be used to harm the student.

The campaign should not require students to download any kind of file on their computer. Doing so could result in unnecessary concerns from the students, as they might believe that their computer has been infected.

Finally, when the student has fallen for the phishing campaign this student has to be notified immediately. This must be done by redirecting the student to a landing page explaining the phishing campaign.

## 2.5 Data Processing

The analysis of the data will be done in GoPhish, as this tool offers detailed information about the users and their behaviour. It is possible to see how many mails have been sent, how many people have clicked the link in which browser and from which location.

More about the results of the analysed data can be found in “5.1 Campaign results”

# 3. Methodology

During the project several phishing topics have been researched, the results of the various studies have been included and processed during the project. Both the research and their processing are elaborated below.

## 3.1 GoPhish

Version v0.11.0 of the GoPhish framework will be used to simplify the setup and execution process of the phishing campaign. GoPhish does this by dividing the phishing steps in several sections within a simple to understand user interface which allows people to launch phishing campaigns with minimal effort. With the use of a borrowed Ubuntu 20.04.3 LTS server from the Rotterdam University of Applied Sciences the GoPhish will be configured and hosted. This will be done by using the instructions in the GoPhish User Guide and with the help of online tutorials. (GoPhish, 2012)

## 3.2 Domain

The setup process of the domain is starting after the completion of the configuration of the GoPhish framework. The domain name will be purchased from the domain registrar Namecheap and for the configuration of this domain name, the A-records are pointed to the Ubuntu server so that it will be reachable.

## 3.3 SSL

To complete the setup of the GoPhish framework, the configuration of SSL for the domain is essential. This will be done by making use of the SSL certificate authority named ZeroSSL.
The configuration will be done through the following steps: selecting the certificate alongside with the domain name, following the verification process displayed by ZeroSSL, and finally downloading and installing the certificate on the server.

Due to prior knowledge and the simplicity of the CNAME verification method, the verification method that will be used is CNAME verification. This verification method requires a CNAME record on the domain with a value that was given by ZeroSSL. Once this record is set up, the certificates will be downloaded from ZeroSSL and uploaded to the Ubuntu server. Finally, for the completion of the SSL configuration, the certificates need to be configured on the server by editing the configuration file of the GoPhish framework. (ZeroSSL, n.d.)

## 3.4 Website

One of the essential parts of the phishing campaign is the website. The goal is to build a web application based on a student shop concept. This has to be done with no prior knowledge of GoPish and it's usage. For the connection between the website and the framework, more research will have to be done. The priority is to use a React web application and try to connect that to GoPish, and if this fails switch to a backup plan of using a simple HTML template which is build up using HTML5, CSS 3 and Bootstrap 4.1.0 and connecting it to GoPish which will be hosted on the Ubuntu 20.04.3 LTS server. The Website must consist of a single page containing the following sections: About Us, Products, Reviews, FAQ and Registration. These sections must also include identifiable markers. Furthermore, the registration section must have the following input fields

* First name
* Last name
* College email
* Password
* Password confirmation
* College institution

These input fields will be used to collect information of the target audience who fall for the phishing attack. For privacy and security reasons the passwords will not be saved.

## 3.5 Six principles of influence

These principles will both be researched and applied within the website and email template, to ensure that students are properly influenced and enticed in falling for the attack. These 6 principles are reciprocity, consistency, social proof, liking, authority and scarcity.

For the email reciprocity, liking and scarcity principles were incorporated. The email starts by sympathizing with the students and how hard they have it (liking). It is then told that the students will be rewarded with great discounts on the products from the webshop upon registering (reciprocity). The products are also chosen to be in limited supply (scarcity) along with having fake reviews to include social proof.

# 4. Campaign

The campaign is based around a fake discount offer for students, where students can purchase expensive electronics with high discounts through a fake webshop. All they have to do is follow the link sent to them by email, where they will be required to register an account in order to purchase the products.

A sense of authority will be created by using a professional looking layout for both our website and email. To create a sense of urgency, the discount offer will supposedly expire after one week. This will hopefully convince students to visit our website sooner rather than later, allowing us to trick more students during the campaign.

## 4.1 Email

The campaign starts with an email where the students will receive a message that informs them about the webshop and tries to convince them to click on a link that leads to the website.

The main focus of the email will be the extra discount students can use when they register on our website. The email features various discounts that demonstrate just how high the discounts can get. To create a sense of urgency, the email will emphasize the fact that the discounts are only available for a week.

To build up trust, the email will contain text to emphasize the problems of the students. For example, it will talk about how hard a student life is and that the store’s owners understand the struggles of the students.

## 4.2 Website

If a student is tricked by the email into clicking the included link to the website, they will then be presented with the campaign’s second layer; the webshop.

The website’s only page will prominently feature the current student discount offer described in the email. To further entice students to register, a featured product will be shown next to the offer with a particularly high retail price and discount.

The website will feature a search bar at the top of the page. This search bar will be nonfunctional.. The footer of the website will feature links to our store’s Privacy Policy and Terms and Conditions pages, but those links will not work either.

Scrolling down, students will see the other products our store sells. When students try to click on a product, the page will scroll down to a registration form.

A false sense of social proof will be created by several product reviews that appear on the frontpage. These reviews will be mostly positive in an attempt to trick students into thinking that our website is trustworthy.

## 4.3 Account Registration

Students will be asked to register an account when they try to purchase a product or view all products. They will be shown a registration popup that asks for the following user information;

* The student's full name,
* The student’s school email address,
* A password,
* The school the student is attending

Only the entered email address will be recorded for statistical purposes. The other information will not be saved, and will therefore be lost the moment the student leaves the page.

After submitting the form, the user will be redirected to a special page that informs the student that they’ve fallen for a fake phishing attack.

## 4.4 Identifiable markers

Both the email and website will feature various hidden identifiable markers that will arouse suspicion in students when spotted. Security-aware students will notice these markers and realize that both the email and website are fake.

The following markers will be hidden in the email;

* Several grammatical and spelling errors will be hidden in the text.

The following markers will be hidden in the website;

* The website’s search function will not work.
* Links to a Privacy Policy and a Terms and Conditions page will be placed in the website’s footer, but both will not work.
* The products listed on the website will be priced at a fraction of the retail price. Perceptive students will realize that these prices are too good to be true.
* Fake student reviews, with clearly fake names such as "Vladimir gnihsihp".
* Fake address which clearly doesn’t belong to any company.

In addition, both the website and email will feature a phone number that looks valid at a glance, but actually uses a nonexistent area code. This makes the email and website look more authentic without the risk of students calling a stranger’s phone number. Perceptive students may also spot this fake telephone number, providing them with another hint that shows this campaign’s true purpose.

Both the email and website will also feature various spelling and grammatical errors. It’s important that there aren’t too many of these errors in the texts, as otherwise it will be too obvious that our website and email are fake.

## 4.5 Informing victims

After filling in the registration form on the website, the victim will be brought to a special landing page. On this page the victims will be informed that they fell for a phishing scam and that they shouldn’t trust random mails with registration information.

 Most of the time, people aren’t aware that there is a lot of data that can be saved on the internet. A section of the page will therefore be dedicated to explaining what malicious things criminals could’ve done using the data that the students entered:

* Using their email address and password, criminals could have logged into and hijacked other accounts that use the same login details. Students will also be recommended to start using a password manager.
* The student’s information could’ve been sold to third parties, who then use it for their own phishing campaigns and other malicious activities.
* The data could’ve used the data to commit identity fraud.

The page will make it very clear that none of the personal information the students have entered has actually been saved, except for the student’s email address which will be used for statistical purposes.

There will also be an email address that students can use to contact us should they have additional questions or concerns about the campaign.

Finally, the page’s footer will state that this phishing campaign was executed as part of the Security Awareness project from the Security Lab minor, and was done with approval of FIT.

# 5. Results

## 5.1 Campaign Results

The campaign was launched on Oct 26, 2021, at 12:32. A total of 239 emails were sent out. The following graph shows the campaign’s results for each day of its runtime;



The final result is that out of 239 students, 27 (11%) clicked on the link, of which 12 (44% of students who clicked the link, 5% of the total) then also submitted data. These results are significantly lower than expected. Research has shown that people between the ages of 18 and 25 are more susceptible to phishing attacks (Sheng et al.), and the majority of the students fall into this age group . Despite this, very few students actually fell for the phishing campaign.

It is important to note that our email did not include a tracking image, as this option was accidentally skipped when the campaign was launched. As such, it is not known exactly how many students actually opened and read the email. The only thing that is known for certain is that the students who visited our website must have also read the email, as they couldn’t have visited the website otherwise. Because this data is incomplete, it was omitted from this report.

One interesting piece of information is the country the students were supposedly located in when they visited our website. While the majority of students were located in the Netherlands, according to *GoPhish*’s Targets Map, several requests originated from the following countries;

* The United States of America
* The United Kingdom
* Russia

While it’s not impossible for some of those students to be international students who actually live in those countries, it is likely that at least some of those requests were made by students using a VPN. At the very least, the request that came from Russia was definitely made using a VPN, as the IP address the request originated from belongs to the popular VPN provider *NordVPN*. According to the data collected by *GoPhish*, the student using this VPN did not submit any data.

5.2 Survey Results
Towards the end of the campaign, a survey was sent out to all students who submitted data. This was done in order to gain some more insight on the campaign’s overall effectiveness and to gather information about how and why the victim fell for the trap.

The survey contained the following questions;

* What convinced you to click on the link?
* What made you fill in your personal information on the site?
* Were you suspicious before clicking the link? Or before entering your personal information?
* What did you learn from this phishing experience?
* Did you notify your fellow students about this phishing campaign?
* Do you have any closing remarks?

Unfortunately, out of the 12 students that were contacted, only one actually responded. Despite this, their response was still very useful.

As it turns out, this student (and likely others as well) told their peers about the campaign after finding out about the security awareness test. It is assumed that because of this, word of the test soon spread throughout the university. This is likely the primary reason the results were significantly lower than originally expected. Considering this student was also one of the first to submit data (doing so only an hour after the campaign’s launch), this would mean that many students would’ve already known about the campaign before even realizing that they received an email.

They also mentioned that while they didn’t fully trust our store due to the unrealistic product pricing and that they couldn’t find us by searching on Google, they still decided to trust us and submit their data. They stated that they did this solely because the phishing mail was sent to their university email account, and they thought that this was an initiative backed by the university. This is a perfect example of the implicit sense of authority one can get by merely sending an email to an email account provided to students by the university instead of their personal accounts.

# 6. Recommendations

As the phishing email did not include a tracking image, it is unknown how many people opened the email and recognized it as a phishing email. It is therefore recommended that a second phishing campaign (this time with a tracking image) is executed at a later time in order to get all the possible data that is needed for proper results.

It might also be beneficial to execute this same campaign again, but with a different target audience. The resulting data of these additional runs may then prove useful in determining what caused the low results from this campaign. For example, if the results of the additional runs end up being significantly higher, it would indicate that the students of the Logistics Management and Automotive courses are more security-aware than originally expected.

As previously mentioned, it would be a good idea for all the universities (in this case the Rotterdam University of Applied Sciences) to start a teaching campaign to keep students up to date with all the possible scams out there related to security and public data theft. This can be done in various ways such as presentations, monthly emails or yearly workshops to each university year and for all studies. This teaching campaign will of course lower the conversion rate for future phishings campaigns, but the more informed students the better.

It could also be an idea to execute a phishing campaign targeted at teachers and other faculty members, to educate them about phishing as well. The login details of teachers are much more valuable than students and it can lead to a catastrophic result if a hacker manages to capture them and thus gain administrative access to the university’s websites.

Another idea would be to send a phishing email to small subsets of many different university courses instead of targeting all students of a specific course. Students from different courses are unlikely to interact with each other, and word of the campaign won’t spread nearly as far if only a small number of students of each course received a phishing email. This would significantly reduce the chance of a student being informed about a phishing campaign before getting the chance to read the email themselves.

#

# 7. Conclusion

The phishing campaign was a success and a lot was learned during its creation and execution. The goal was to test the security awareness of students from the Logistics Management and Automotive bachelor studies, which were also our target audience. With the help of a program called GoPish, a phishing campaign was set up. This consisted of creating a landing page and a mail template. It was decided that the landing page would consist of interesting and thoughtful things which would entice students of the target audience to click on the products. Upon clicking on these products the students would be asked to register, after which their sensitive data would be saved (excluding their password). After the students submitted their data on the registration page, they were then directed to a page which informed them about the security awareness test, and contained information about the risks of falling for such an attack. This landing page is meant to inform all the victims that such an attack could have been real and would have real life consequences, if it would have been a real attack.

It was interesting to be able to look at the data which was setup in GoPish regarding views and clicks. Unfortunately, no tracking image was added in the email template which resulted in loss of information regarding how many students clicked on the email. This results in missing data on the conversion rate from views to students clicking on the website. This will remain a big learning point for the future and needs to be focused on for future campaigns. The survey was sent to both study groups and would have yielded valuable information if they were filled in, but unfortunately this wasn't the case.

However, it is safe to say that the victims which did fall for the attack have been informed properly and this is a win-win for both parties.

# 8. Document information overview

## Revision history

| **Date** | **Changes** |
| --- | --- |
| Oct 27, 2021 | Set up document outline |
| Oct 28, 2021 | Add introductionStart writing ResultsMinor changesExecutive summary setup |
| Oct 29, 2021 | Minor formatting changesStart on Methodology and result (short)More work on ResultsStart writing Recommendations |
| Oct 30, 2021 | Finish ResultsFinish RecommendationsAdd scope |
| Nov 16, 2021 | Reworking chaptersAdding informationBetter introduction |
| Nov 22, 2021 | Campaign limitations improvements |
| Nov 23, 2021 | Final adjustments  |

##

# 9. References

GoPhish. (2012). *Documentation*. Documentation - GoPhish. https://getgophish.com/documentation/

Juma, A. (2015). *The 6 Principles of Influence: How To Master Persuasion*. Medium. https://alyjuma.medium.com/the-6-principles-of-influence-how-to-master-persuasion-2f8c581da38b

Sheng, S., Lanyon, M. B., Kumaraguru, P., Cranor, L., & Downs, J. (2010, January). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*. https://www.researchgate.net/publication/221514257\_Who\_falls\_for\_phish\_A\_demographic\_analysis\_of\_phishing\_susceptibility\_and\_effectiveness\_of\_interventions

ZeroSSL. (n.d.). *Quick Installation*. Quick Installation - ZeroSSL. https://zerossl.com/features/installation/