



**Gophish**

# Reviews, tips, and advice from real users



Powered by  **PeerSpot**

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 14

ROI..... 15 - 17

Use Case..... 18 - 21

Setup..... 22 - 24

Customer Service and Support..... 25 - 26

Other Advice..... 27 - 30

Trends..... 31 - 32

About PeerSpot..... 33 - 34

# Product Recap



Gophish

# Gophish Recap

Gophish is an open-source phishing toolkit aimed at simplifying the creation and execution of phishing campaigns for cybersecurity professionals.

Designed to cater to organizations seeking to enhance their security awareness, Gophish offers a streamlined process for launching phishing simulations. It provides a customizable environment, allowing users to simulate real-world phishing scenarios efficiently. With its user-friendly interface, even those with limited technical skills can easily navigate and deploy effective campaigns. Gophish has become a vital tool for companies looking to test employee susceptibility to phishing attacks and refine their security protocols.

## What are the key features of Gophish?

- **Campaign Automation:** Automate phishing campaigns with pre-designed templates and schedules.
- **Customizable Landing Pages:** Easily create and edit landing pages to closely mimic real phishing sites.
- **Real-time Reporting:** Obtain immediate results and insights for each campaign to assess effectiveness.
- **User Management:** Organize targets into groups for specific and detailed phishing simulations.

## What benefits and ROI can users expect?

- **Enhanced Security Awareness:** Users gain valuable insights into employee responses to phishing attempts.
- **Cost-effective Training:** Reduces the need for expensive external security consultants.
- **Improved Incident Response:** Helps organizations develop more robust protocols against security threats.
- **Scalable Solutions:** Easily manage small to large-scale campaigns with minimal operational impact.

Gophish is widely adopted across banking, healthcare, and retail industries to tackle specific challenges related to phishing risks. In banking, it helps simulate threats that target customer financial information. Healthcare organizations leverage it to protect sensitive patient data by educating staff to recognize phishing attempts. In retail, Gophish assists in safeguarding consumer transaction data. Its adaptability and effectiveness make it a favored choice for diverse industry needs.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “The impact it has had is that we have been able to sell it to clients who, for example, do not have the money to pay for a platform because they are small startups, and so with Gophish we create a solution that is cheaper for them.”



**Juanfran Celdran**

Administrador de sistemas informaticos en red at a consultancy with 201-500 employees

- ✓ “Gophish has had a positive impact on my organization, as I noticed that since I used Gophish for the benefit of several clients, the maturity level of my clients was increasing.”



**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

- ✓ “The best feature that Gophish offers is its customizability; it makes everything look very professional and makes tracking very easy.”



**Rocky Yuan**

Senior Offensive Security Engineer at a computer software company with 1,001-5,000 employees



“Overall, Gophish is dependable for phishing simulations and awareness assessments.”



**Avidévan Kandagiri**

Cyber Fraud Analyst at a security firm with 201-500 employees



“Regarding my use of Gophish in this academic context, I found it extremely easy to use; you do not need to be a technical person with special skills to be able to handle it.”



**Faiza Haddadi**

student at a comms service provider with 1,001-5,000 employees



“Gophish has positively impacted my organization by making it very easy to set up and start phishing campaigns.”



**Anass Bekar**

Senior Offensive Security Engineer at Secmund



“Gophish has positively impacted my organization by increasing awareness among my employees.”



**MohammedJaffir**

Founder at Cipheroot Cybersecurity Solutions

## What users had to say about valuable features:

“The best features Gophish offers are that it is user-friendly and easy to use. Its user-friendly interface helps me in my daily work by making setup quicker.

Gophish has impacted my organization positively in terms of security awareness. I have noticed fewer phishing incidents and more responses towards reporting phishing emails as specific improvements. .”

### Verified user

Senior Information Technology Auditor at a tech vendor with 10,001+ employees

[Read full review](#) 

---

The main point of Gophish is the automated sending, as I can send to several email addresses at once by uploading a list of emails.

I also consider the SMTP configuration of the server from which I send the emails to be a differentiator because it is very simple to do.

“With Gophish, I am able to work in a more appropriate way on phishing awareness, and I am also able to make employees aware in an easy and appropriate way because they see how a phishing attack works in a real way. This allows them to become aware in a more practical way.

“I did notice a measurable change as employees are more aware of phishing and the number of incidents has decreased because they now know how phishing works. .”

### VINICIUS DA SILVA

analista de segurança da informação at a financial services firm with 201-500 employees

[Read full review](#) 

“The best feature Gophish offers in my experience is the learning part. You can set it up on your own and learn new things by practicing and thinking from an attacker's perspective. What do they think? How do they deliver the payload, the mails? I think that part is the best. The UI is definitely very friendly.

What makes Gophish's UI friendly for me is the layout. Every step on the left panel, I can see. I just have to go to the next step, and I can even edit my previous step. The UI is very friendly in the sense that I don't have to navigate to different dropdowns or panels. Regarding the attacker's perspective, it really helps in thinking about how real-life fraudsters and attackers set up their own servers and try to mimic phishing attacks.

Gophish has helped in strengthening the relationship with our clients. It has also helped us give training regarding simple social engineering and phishing attacks that every employee must follow. For example, not clicking any suspicious mail. People know about it but they don't follow it. An actual real-life example where they are given a phishing mail out of the blue and they are clicking it gives us an idea of what people do when they're not being watched. That really helped us set up statistics and was very helpful..”

**Avidevan Kandagiri**

Cyber Fraud Analyst at a security firm with 201-500 employees

[Read full review](#) 

“The best features that Gophish offers, the ones that impressed me the most during my use, are mainly two things. The fact of having templates makes the task easier instead of creating an email and copy-pasting for each person every time. Here, you can create campaigns and send them, and you can create a CSV file, for example, and send directly to all the people you list there, so it saves time.

“Also, the dashboard gives a direct view of the clicks and the number of people who received the email, making it very illustrative and saving from having to compile the results manually, delivering them in Excel tables or whatever; it is directly visible in the application, and it is easier to read that way.

“Gophish has had a positive impact on my learning and my academic path in cybersecurity as it allowed me to understand and go deeper into the concepts of social engineering and phishing attacks. It gave me experience because this is a project I completed and published on GitHub, and there were even other students who were interested and contacted me for information. This is a project that I added to my CV, and I am very happy, not just because I added it to my CV but because it allowed me to learn things..”

**Faiza Haddadi**

[Read full review](#) 

student at a comms service provider with 1,001-5,000 employees

---

“The best feature of Gophish is that it makes phishing simulation very simple and practical. First, it allows us to create realistic email templates. We can design emails resembling password reset alerts, HR notifications, invoice emails, document sharing, or account verification messages. Second, it supports landing pages, so when a user clicks the link, we can direct them to a safe awareness page or a simulated login page to understand their response. Gophish also allows landing pages to be created or imported and connected to each campaign. Another strong feature is campaign management, which is easy to manage. We can create user groups, select an email template, choose a landing page, configure the sending profile, and launch the campaign in a structured way. Another strong feature is tracking; Gophish helps us see who opened the email, who clicked the link, and who submitted the information during the campaign. This is very useful for measuring employee phishing awareness and risk levels.

“Gophish has positively impacted my organization by increasing awareness among my employees. Before using security awareness training with Gophish, the phishing clicking rate was seventy-five percent; now it has reduced to twenty percent.

“It takes us a month to see this improvement, and we train our employees on how phishing works and how attackers will deceive information from them. We also simulate this kind of activity through Gophish. After doing this, employees are getting awareness on phishing every month.

“My most favorite features are landing pages and reporting because it is very useful for me to create a landing page, and we can track how employees behave regarding that link..”

**MohammedJaffir**

Founder at CIPHERoot Cybersecurity Solutions

[Read full review](#) 

“In my opinion, the best features of Gophish are recipient management, template creation, detailed reporting, and the API.

Recipient management makes it easy to organize target groups by client, department, user profile, or risk level. This helps prepare campaigns that are better adapted to each specific context.

The email and landing page templates are also very useful because they allow realistic and contextualized scenarios to be created. This level of customization makes campaigns more relevant and helps assess how users react to situations that are close to their real working environment.

I particularly appreciate the reporting capabilities, as they help measure campaign effectiveness and the client’s maturity level. Gophish provides key indicators such as email open rates, click rates, data submission rates, and behavioral changes across multiple campaign iterations.

The Gophish API is another strong feature. It makes it possible to automate several tasks, including campaign creation, email delivery, result collection, and integration with cybersecurity awareness platforms or other internal tools.

Another major advantage is that Gophish is open source and free, which makes it accessible, flexible, and easy to adapt to different organizational needs.

Gophish has had a positive impact on my work with several clients. For example, during an initial campaign, more than 70% of the targeted employees submitted data. After a contextualized awareness training session, we launched a similar campaign again, and the data submission rate decreased to around 40%. This improvement showed a clear increase in employee awareness and maturity regarding phishing risks..”

**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

[Read full review](#) 

# Other Solutions Considered

I evaluated some options on the market before choosing Gophish, but the cost was very high. I chose Gophish because it has a relatively low cost and features that are more appropriate for what I need on a daily basis.

## VINICIUS DA SILVA

analista de segurança da informação at a financial services firm with 201-500 employees

[Read full review](#) 

---

“Before choosing Gophish, I evaluated options such as King Fisher, Evilginx, and the B4, but I found that Gophish was an open-source and readily available tool with very little costs and also the flexibility of using my own templates..”

## Verified user

Senior Information Technology Auditor at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“Before using Gophish, we used KnowBe4, which is also similar to Gophish, but KnowBe4 has additional features, such as providing video training courses. If the user clicks the phishing link, they receive a banner stating, "You are hacked. You clicked the phishing link," which helps users understand why they clicked and what they clicked on..”

## MohammedJaffir

Founder at Cipheroot Cybersecurity Solutions

[Read full review](#) 

“Before using Gophish, I did not test other similar solutions; I chose Gophish because I had downloaded a list of cybersecurity projects to do, and among those projects, there was a phishing attack simulation project suggesting the use of Gophish. That is how I discovered Gophish, and I did not think about looking for or using other tools since Gophish met my needs..”

**Faiza Haddadi**

student at a comms service provider with 1,001-5,000 employees

[Read full review](#) 

---

“I was not using a similar solution before adopting Gophish. We selected Gophish directly after conducting a comparative study more than three years ago.

At that time, we evaluated several competing solutions, although I no longer remember the exact names of the tools that were assessed. Gophish stood out for several reasons: it is open source, free to use, well documented, and relatively easy to install thanks to the available resources and community feedback.

Another important selection criterion was the availability of a fairly complete API. This allowed us to integrate Gophish with other internal tools and automate certain tasks related to cybersecurity awareness and phishing simulation campaigns.

In the end, we chose Gophish because it met our functional needs while offering an excellent balance between flexibility and cost..”

**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

[Read full review](#) 

“Before choosing Gophish, we evaluated several competing solutions as part of a comparative study. However, since this analysis was conducted more than three years ago, I no longer remember the exact names of the tools that were assessed.

The main comparison criteria were cost, ease of installation, availability of documentation, solution flexibility, integration capabilities, and the level of automation supported.

Gophish stood out mainly because it is open source, free to use, and well documented. The absence of licensing costs was an important advantage. The available documentation and community resources also made installation and onboarding easier.

Another major advantage of Gophish was its API, which provided enough capabilities to integrate it with our internal tools and automate certain stages of the campaigns, including preparation, execution, and result collection.

Compared with some commercial solutions, Gophish may require more configuration and administration effort. However, it offers greater flexibility, a much lower cost, and strong adaptability. This balance between cost, simplicity, flexibility, and integration capabilities was the main reason we selected Gophish..”

**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

[Read full review](#) 

# ROI

Real user quotes about their ROI:

“I have seen a return on investment in terms of time saved; building phishing campaigns is much more straightforward, and the setup was acceptable, but with more instructions on the user manual, that would be quicker..”

## Verified user

Senior Information Technology Auditor at a tech vendor with 10,001+ employees

[Read full review](#) 

“There has been a return on investment; we need fewer team members to do the same engagements. Before, you needed three people for an engagement, but now just one person can manage. So there definitely was a lot of money saved..”

## Anass Bekar

Senior Offensive Security Engineer at Secmund

[Read full review](#) 

Regarding return on investment, there is not a typical ROI since Gophish is free and accessible to anyone. The investment is mainly in the time and effort required to learn and integrate it into systems. In terms of relevant metrics, it does not reduce the need for more employees but rather replaces other paid tools, which is advantageous, as it delivers cost savings compared to commercial tools.

**Alaaeddine Elhaoua**

Software Engineer at TechZone LLC

[Read full review](#) 

---

“We have not saved time, but we have saved money because most suspicious links come from spam and junk mail attacking employees and the company's servers. Previously, my clicking rate was seventy-five percent, but it has reduced to twenty-five percent due to Gophish and our training..”

**MohammedJaffir**

Founder at Cipheroot Cybersecurity Solutions

[Read full review](#) 

---

“I have noticed a return on investment in terms of time saved and skills acquired thanks to my use of Gophish. It is thanks to this tool that I was able to carry out these phishing attack simulations, understand how it works, see concrete results, and even make a small slide deck that explains this little project and includes advice that I might present in the future to some users..”

**Faiza Haddadi**

student at a comms service provider with 1,001-5,000 employees

[Read full review](#) 

“Yes, we have seen a return on investment with Gophish, mainly through licensing cost savings. Since Gophish is an open-source solution, there are no licensing fees, which is a significant advantage compared to some commercial solutions.

The main costs are related to hosting the platform, configuring it, and the time spent preparing, monitoring, and analyzing campaigns. Even with these operational costs, the overall cost remains controlled, especially in a multi-client context.

Another positive aspect of the ROI is the gradual improvement in employee awareness. By tracking campaign indicators such as click rates and data submission rates, it is possible to measure behavioral changes after awareness actions.

For example, in some campaigns, we observed a decrease in the data submission rate after contextualized awareness training. This shows that Gophish provides value not only from a cost perspective, but also by helping reduce risky behaviors..”

**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

[Read full review](#) 

# Use Case

“My main use case for Gophish is phishing campaigns. A quick specific example of how I use Gophish for phishing campaigns is for security awareness and training.

I use it for tracking responses, ratings, and also analyze statistics regarding my main use case. .”

**Verified user**[Read full review](#) 

Senior Information Technology Auditor at a tech vendor with 10,001+ employees

---

“My main use case for Gophish is conducting mock phishing drills, which was one of the biggest ethical reasons we can use Gophish for during my previous internship. For those mock phishing drills, we set them up on our cloud, on a virtual machine. From there, we set up all the landing templates. For example, we took a landing page of Netflix and we sent an email through Gophish using a real domain that we had purchased. We sent the mail to the employees of our clients. They ended up opening the email. For 400 employees, we sent 400 mails. The result was that 300 opened the mails and around 15 people actually submitted their information..”

**Avidevan Kandagiri**[Read full review](#) 

Cyber Fraud Analyst at a security firm with 201-500 employees

---

“I used Gophish for a project last August, a phishing attack simulation, and I reused it recently because a student found the project I did on GitHub and wanted to do the same project, so he asked me some questions, and I reused it at that time.

“My main use case for Gophish is in a phishing attack simulation project where the idea is to learn and understand social engineering and how to simulate phishing attacks when you're in a Red Team. I also created a slide deck that explains how to recognize a phishing attack, showing some of the results of the three campaigns, and then at the end, I provided some advice to people to avoid falling for those kinds of phishing attacks..”

**Faiza Haddadi**

[Read full review](#) 

student at a comms service provider with 1,001-5,000 employees

---

My main use case for Gophish is for employee awareness within the company, and I use it for phishing campaigns.

I create emails to raise employee awareness and send them to see if employees end up clicking. If they click, I reach out to them after finishing the campaign and conduct awareness work so they do not fall for phishing.

“I configure Gophish within our Office 365 and proceed with the campaigns, sending emails similar to Microsoft's, emails similar to service providers', and I analyze the results. If someone falls for it, I then handle awareness together with that person. .”

**VINICIUS DA SILVA**

[Read full review](#) 

analista de segurança da informação at a financial services firm with 201-500 employees

---

“My main use case for Gophish is running phishing simulation campaigns for multiple clients of different sizes. I have also used the Gophish API to automate certain phishing scenarios and integrate the tool into a cybersecurity awareness platform.

For example, I conducted a campaign for one of my clients to assess the maturity level and security awareness of their employees regarding phishing risks. We first defined the campaign objectives with the client, then selected the target audience, chose the scenario, and validated the landing page.

The selected scenario involved simulating an email from the HR department. We also reproduced a web page related to the client’s environment to make the exercise more realistic. The goal was to measure employee reactions, identify risky behaviors, and evaluate their overall level of awareness.

For this type of campaign, I use Gophish through its web interface, API, and campaign management features..”

**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

[Read full review](#) 

“My main use case for Gophish is to run a phishing awareness campaign inside an organization in a safe and controlled way. For example, instead of waiting for a real attacker to send a fake email to employees, the company can simulate a phishing email using Gophish. The email may look legitimate or resemble a login alert, password reset request, an invoice, an HR notice, or a document sharing link. The goal is not to blame employees; the goal is to understand how many people may click the suspicious link and enter credentials or report the email to the security team. Based on the results, the company can train employees better to reduce their risk of a real phishing attack. Gophish helps the security team create an email template, landing pages, user groups, and campaigns, and it also shows useful reports such as who opened the email, who clicked the link, and who submitted the information. In simple terms, Gophish is the tool that helps the organization test employee awareness before the real attackers do.

“In my recent campaign, we created a controlled email that looked like an internal password expiry notification. This message informed employees that their password was about to expire and asked them to click the link and verify their account. Some employees clicked it. Using Gophish, we created the email templates, added the target user groups, and connected to safe landing pages. The landing pages did not collect the real password; they were only used to track awareness and show training guidance. After sending the campaign, Gophish helped us measure how many users opened the email, clicked the link, and submitted the details. Based on the results, we identified which department needed more phishing awareness training. The main purpose was not to blame anyone; it was to understand employee behavior, reduce phishing risk, and help the company prepare better against a real attack.

“One challenge I faced was the credential awareness simulation. We set up a phishing campaign where employees received an email that looked like a password expiry or account verification message. The landing page was only for awareness testing; we did not collect the real password or sensitive data. The outcome was useful because it showed which user or team is more likely to fall for phishing. Gophish is very useful because it turns security awareness into a practical exercise. Instead of just telling employees about phishing, we can safely show them how phishing works and help them learn from real-world style scenarios..”

# Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

My experience with pricing, setup costs, and licensing has been great. There are no costs since Gophish is publicly licensed software, and it was easy to implement because there are no costs.

**VINICIUS DA SILVA**

[Read full review](#) 

analista de segurança da informação at a financial services firm with 201-500 employees

---

“My experience with pricing, setup costs, and licensing shows that the setup cost is not very high; Gophish is completely free, as it is an open-source tool..”

**MohammedJaffir**

[Read full review](#) 

Founder at Cipheroot Cybersecurity Solutions

---

“I did not purchase Gophish through the AWS Marketplace; I have installed it manually, only as a server. It is easier to install compared to other simulating tools..”

**Verified user**

[Read full review](#) 

Senior Information Technology Auditor at a tech vendor with 10,001+ employees

---

“Gophish was deployed on our public cloud with a firewall in front of it, so only our IPs were whitelisted, although it was public. In the campaign itself, we put our own domain, and the mails were sent through that domain's mail server. I used Microsoft Azure for deploying Gophish..”

**Avidevan Kandagiri**

[Read full review](#) 

Cyber Fraud Analyst at a security firm with 201-500 employees

---

“Regarding my use of Gophish in this academic context, I found it extremely easy to use; you do not need to be a technical person with special skills to be able to handle it. In maybe an hour or two, I understood how to use it, how to create templates, how it works with landing pages and dashboards. It is really useful and very easy to use, so I recommend it both for cybersecurity students like me and for security professionals..”

**Faiza Haddadi**

[Read full review](#) 

student at a comms service provider with 1,001-5,000 employees

---

“The initial setup of Gophish was generally quite straightforward, although I did face some difficulties at the beginning during the installation process.

These challenges were mainly related to the initial deployment and some configuration settings. However, after reviewing the documentation and using the resources available in community forums, the issues were resolved without major difficulty.

In my opinion, installing Gophish does not require highly advanced expertise, but it does require a solid technical foundation, especially in hosting, network configuration, SMTP setup, and securing access to the platform.

Overall, I would say that the initial setup is fairly accessible for someone with a technical background. It is important to read the documentation carefully, test the configuration before launching a campaign, and rely on the community resources when needed..”

**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

[Read full review](#) 

# Customer Service and Support

“There is no support for Gophish because it is open source, so I have not needed to contact assistance or technical support for this tool.

“We have no contact with Gophish aside from being a customer..”

## Verified user

Ingénieur en Sécurité at a tech vendor with 501-1,000 employees

[Read full review](#) 

---

“Gophish's customer support is not something I investigated deeply since it is an open-source solution. Of course, you have the community on GitHub and many ways to research. There is also Gophish documentation, which I saw exists. However, Gophish is a very intuitive tool, so it does not raise major questions. I did not need any support from their team..”

## Verified user

Analista de Infraestrutura de TI at a tech vendor with 11-50 employees

[Read full review](#) 

“I have never reached out to customer support before. What I normally do is research, sometimes read the documentation, or sometimes go through some YouTube videos to find my way around things instead of contacting support directly. If I do everything that I have already said and it does not work out, the next thing I tend to do is contact customer support. As of now, I have never contacted customer support before..”

**Bright Boateng**

Soc Analyst And Threat Intelligence Analyst at CYBERTEQ

[Read full review](#) 

---

“Gophish support is different from what you would expect from a commercial solution, as it is an open-source tool. Therefore, there is no traditional customer support with a dedicated team or formal service desk.

However, my experience has still been positive because the documentation is clear and detailed enough to resolve most issues. I have never needed to contact technical support, as the available guides and community resources helped me find the answers I needed.

In my opinion, Gophish is well suited for teams with some technical skills that can rely on documentation and community forums. For organizations that require official support, service-level commitments, or direct assistance, this may be a limitation to consider..”

**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

[Read full review](#) 

## Other Advice

My advice to others who are thinking about using Gophish is to use it because it is a very practical tool for running phishing tests, it is very easy to configure, and it is free. I would rate this product a seven out of ten.

---

**VINICIUS DA SILVA**

analista de segurança da informação at a financial services firm with 201-500 employees

[Read full review](#) 

“Regarding Gophish's AI capabilities, I find its governance and security overall acceptable. Regarding Gophish's AI capabilities, I think the accuracy and reliability of output are good. I would recommend others looking into using Gophish to use it for performing their security awareness and campaigns because it is easier to install compared to other simulating tools.

Providing more details and videos on proper tutorials would be helpful. I found this interview to be good; it is well-calibrated and conducted effectively. I would rate this review an 8 out of 10. .”

---

**Verified user**

Senior Information Technology Auditor at a tech vendor with 10,001+ employees

[Read full review](#) 

“My advice for others looking into using Gophish is to explore more. Gophish is a very good tool and can be used within the organization and with clients. If you're catering to your own clients, then you can use it for them as well. My advice would be to start with a small pilot campaign before rolling it out across the organization.

That would help you validate any small hiccups that you come across. Gophish is relatively easy to deploy and use, and you can create realistic templates and use it to improve the results.

Regarding Gophish's AI capabilities, I don't think it is an AI-driven platform, so I haven't evaluated it based on AI-generated content. From my experience, the platform is very reliable in terms of campaign management and email delivery tracking and reporting, including the clicks. Overall, Gophish is dependable for phishing simulations and awareness assessments.

I rate Gophish a nine out of ten. I would choose nine out of ten because of how easy it is to set up. What makes it different for me not giving it a ten is the education part, as we can add training modules that would really help the organizations using Gophish for phishing drills because they can simply direct them to links that show what they need to do..”

**Avidevan Kandagiri**

Cyber Fraud Analyst at a security firm with 201-500 employees

[Read full review](#) 

---

“I would rate Gophish **9 out of 10**.

My advice to organizations considering Gophish is to start by properly securing the platform installation. It is important to use HTTPS, protect access to the administration interface, and restrict access to authorized users only.

Before launching a phishing simulation campaign, it is also essential to clearly define the objectives, validate the scenario, run preliminary tests, and carefully select the target audience. An effective campaign should be contextualized and aligned with the organization’s maturity level.

I also recommend paying close attention to data management. Campaign results

may contain sensitive information related to employees or clients. Therefore, it is better to limit data retention and delete campaign-related data after completion, in accordance with confidentiality requirements and internal policies.

Overall, Gophish is a very effective, flexible, and cost-efficient solution for running phishing awareness campaigns, provided that campaigns are properly prepared and the environment is securely configured..”

**Rabah AROUDJ**

Senior Cybersecurity Consultant at Mare Nostrum Advising Groupe

[Read full review](#) 

---

“A good template helps measure whether employees can identify suspicious links, sender issues, and urgency-based messages, which has very much surprised me.

“Regarding Gophish's AI capabilities, I see it mainly as a phishing simulation tool, not a fully-fledged AI platform. For governance and security, I believe the key is responsible and authorized use; campaigns should be approved, access should be limited, employee data must be protected, and results should be used for awareness training, not blaming people. If AI is used to create a template or analyze results, human review is important to ensure the content is safe, ethical, and aligned with company policy.

“Gophish is reliable for tracking campaign results such as opens, clicks, and submissions, but it is not mainly an AI-based tool. If AI is used to generate a template or analyze results, I would not trust the output blindly. AI can be useful, but it should be treated as a draft; a human should review the content for accuracy, tone, company policy, and ethical use before launching any campaign.

“I advise others looking into using Gophish to use it safely with authorization and permission from your company to avoid unauthorized access and misuse, as misuse could lead to severe consequences. I would rate this product nine out of ten..”

“In my opinion, the one I found most interesting was the one from CROUS because generally when students arrive here in France and they see this, they have to pay quickly since phishing attacks usually use an urgent tone. Since these students are afraid of losing their CROUS housing, they might quickly pay, just click on the link and proceed with the payment without necessarily realizing that it is a scam, especially since generally, people who come from certain African countries do not really have this concept of scam and phishing.

“The project is purely academic; I did it with fake email addresses that I managed with Mailpit. I created fake emails that do not exist, for people who do not exist, and I was the one who clicked on these emails myself, opened them, or accessed the links in the attachments of each email. Again, it was purely for academic purposes so I could learn because otherwise, with real email addresses, I cannot really do that, and also it is a bit complicated with Gmail. I preferred to do it with Mailpit and fake email addresses.

“Regarding campaign management and the use of templates, Gophish's interface seemed very intuitive to me from the start; everything was clear and self-explanatory. You have buttons for each thing, and it does not really require super advanced knowledge; it is very easy to handle.

“I do not really have any improvements in mind at the moment, but offering ready-made templates that we could use or examples of emails that we could directly use would be beneficial.

“I do not have any particular advice for other people who want to use Gophish in an academic or professional context; I would tell them to go for this tool because it is really easy to get started with. You do not need to be an expert to use it, and it helps a lot with dashboards and templates. My overall rating for this product is 9 out of 10..”

**Faiza Haddadi**

student at a comms service provider with 1,001-5,000 employees

[Read full review](#) 

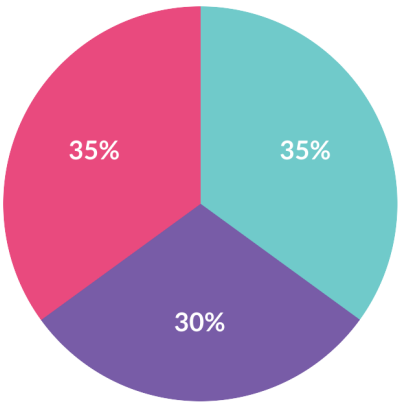
# Top Industries

by visitors reading reviews

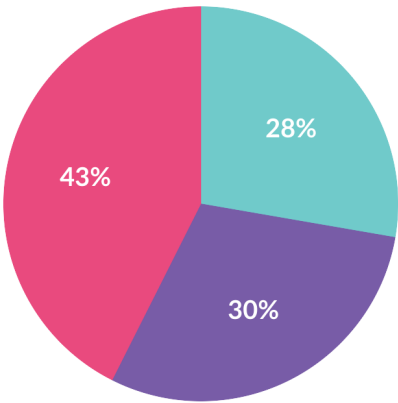


# Company Size

by reviewers



by visitors reading reviews



Large Enterprise      Midsized Enterprise      Small Business

# About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

## Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

# About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: [www.peerspot.com](http://www.peerspot.com)

## PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944