

# Say NO to Phishing

Guide by 3Gi Internet Services



FREE Download

# What is phishing?

Phishing is a type of online scam where criminals send out fraudulent email messages that appear to come from a legitimate source.

The emails are designed to trick the recipient into entering confidential information (ex: account numbers, passwords, pin, birthday) into a fake website by clicking on a link.

The email includes a link or attachment that, when clicked, will steal sensitive information or infect a computer with malware.



Phishing involves tricking people into giving out sensitive information or passwords. It's called PHishing due to a long-time hacker tradition of using "PH" in place of "F".

# Types of phishing attacks



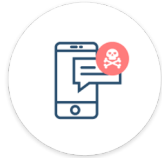
## Clone Phishing

Clone Phishing is where a legitimate and previously delivered email is used to create an identical email with malicious content. The cloned email will appear to come from the original sender but will be an updated version that contains malicious links or attachments.



## Spear Phishing/Whaling

Spear Phishing is a more targeted attempt to steal sensitive information. It typically focuses on a specific individual or organisation. These types of attack use personal information that is specific to the individual in order to appear legitimate.



## Vishing/Smishing

Vishing refers to phishing scams that take place over the phone call. This type of attack involves the most human interaction, but it follows the same pattern of deception as other types of phishing attacks.

Smishing is a type of phishing that uses SMS messages as opposed to emails to target individuals

# What are your risks?



## In Your Personal Life

- Money stolen from bank accounts
- Fraudulent charges on credit cards
- Tax returns filed in a person's name
- Loans and mortgages opened in a person's name
- Loss of access to photos, videos, files, and other important documents
- Fake social media posts made in a person's accounts



## At Work

- Loss of corporate funds
- Exposed personal information of customers and co-workers
- Outsiders gain access to confidential communications, files, and systems
- Files become locked and inaccessible
- Damage to employer's reputation

# What to look for?



Please pa..

## Please pay overdue toll


**EP** EasyPay Support — Sender Name and Domain Spoof Known Brand  
to AP@yourcompany.com

Notice to Appear, — Impersonalized Messages

You have not **paied** for driving on a toll road and the **fee is past due.** — Grammatical Errors

The copy of the invoice is attached to this email. — Scare Tactics

Best Regards,  
John Doe  
EasyPass Agent — Imitating a Known Brand

 ZIP E-ZPass\_0000300019.zip — Compressed Attachments

# How to protect yourself against phishing attacks



- Never click on suspicious links
- Do not reply to suspicious emails
- Be careful what you post online
- Verify the security of websites
- Be vigilant while downloading email attachments to your computer. If in doubt, do not download



**If you think you've received a phishing email,  
report it to support@3gi.co.za**



[www.3gi.co.za](http://www.3gi.co.za)