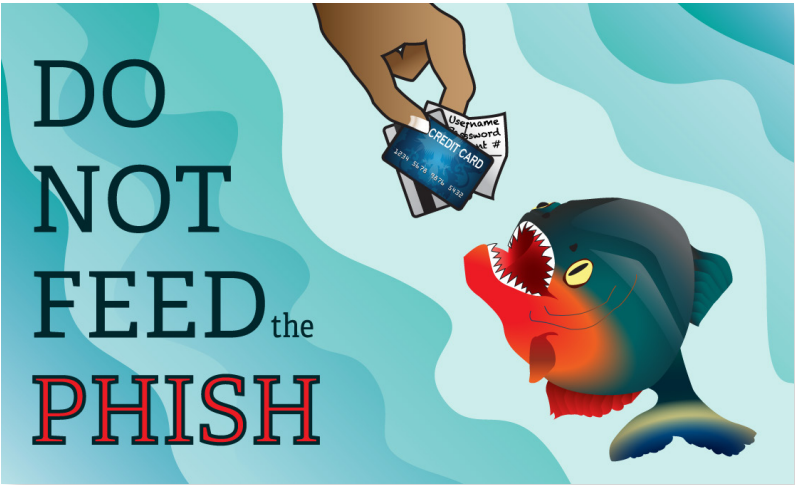


Lets talk about **Phishing**...

No, not the activity involving a rod, bait, an expanse of water, whiskey and maybe even some actual fish.....

We are talking about **“Phishing”** with a **“Puh Huh”** and not a **“Ffff”**.



Phishing is **the attempt to obtain sensitive information** such as **usernames, passwords, and credit card details** (and sometimes, indirectly, **money**), often for **malicious reasons**, by masquerading as a **trustworthy entity in an electronic communication**.



In its simplest form, a Phishing email will **typically direct the user to visit a website where they are asked to update personal information**, such as a password, credit card, social security, or bank account numbers, **that the legitimate organization already has**.



The website, however, is **bogus** and will **capture and steal any information the user enters on the page**. You may not think the website is bogus, as **these guys are really good at impersonating the look and feel around a banking site**. People far cleverer than you have been caught before, so **you need to be really vigilant**.

“The Hover Test”

If you receive an email with a hidden link such as **“Click Here”**, do the hover test.



Hover your mouse over the link and look at the lower left pane to see where the link leads. Does it look legit?

Are they directing you to go to:
“freemedicalstuff.com/stuff/morestuff/getidiottochangedetails.html”
when you are expecting to change your FNB bank details?

Follow these additional tips to avoid being a phishing victim:

- **Do NOT click links in messages that ask you to log in.** Type a trusted Web address in your browser or Google for the Web site if you don’t know the address.
- **Never type personal, sensitive information** (such as passwords or account numbers) on Web sites without verifying the Web site’s authenticity and security — look for an **“https”** in the address bar.
- **Verify the address.** Malicious web sites may look identical to a legitimate site, but the address may use a variation in spelling or a different domain (.com vs. .edu).
- Misspellings and grammatical errors can be a dead giveaway in phishing emails and subject lines.
- If you are unsure whether a request is legitimate, **contact the company directly**. Do NOT use contact information provided in the request.
- Don’t open attachments. They may contain viruses or malware that can infect your computer.
- Protect your password. Information security and IT officials should never ask for these details.
- Report suspicious activity. If you have any questions or you receive a suspicious email that you want to report, let your local IT bloke know.



A word from the world of IT
George, Lightstone Group Technology Officer