 **Phishing** 

**What is Phishing?**

[Phishing](http://uk.norton.com/security_response/phishing.jsp) (pronounced "fishing") is a kind of identity theft which is growing in popularity amongst hackers.  Hackers are highly skilled computer experts capable of breaking into [computer systems](https://en.wikipedia.org/wiki/Computer) and [networks](https://en.wikipedia.org/wiki/Computer_network) even the ones which are highly secure. By using false websites and emails, they attempt to steal your personal data - most commonly passwords and credit card information.

Criminals gain this information by sending you links to sites that look like sites you trust, such as your online banking provider or social networks, and are able to steal your data as you enter it. Some of the sites which turn out to be victims most regularly include PayPal, eBay, Yahoo! and MSN as well as financial institutions - so don't think that an email is guaranteed to be safe when it's not from a bank.

 

**How to protect yourself against phishing?**



1. Be aware of emails asking for **confidential information** - especially financial information like bank details. Legal organisations and companies will never request personal information via email, and most banks will tell you that they won't ask for your information unless you're the one contacting them.
2. Don't get nervous and fall into their trap! Phishers like to use **scare tactics**, and may threaten to disable your account or delay services until you update certain information. Be sure to contact the owner directly to confirm the authenticity/originality of their request.
3. Make sure you read the website's **privacy policy well**. Majority of commercial websites have a privacy policy, which is usually seen at the bottom of the page.

**If most of the spam/fake emails you receive are on a daily basis, it’s because you have signed up to a website and given your email address to another company. If you're not ok with this happening, it might be worth reconsidering whether you want to sign up to the site.**

1. Many phishing emails begin with "Dear Sir/Madam", and some come from a bank with which you don't even have an account. So think twice before you click and agree to provide your details.
2. Never submit confidential information via **forms** along with the email messages. Senders are often able to track all information entered.



1. Never use links in an email to connect to a website unless you are absolutely sure they are not fake. Instead, open a new browser window and **type the URL directly** into the address bar.
2. Make sure you maintain effective **anti-virus** **software** installed in your computers to fight against phishing.

 For example: Norton Internet Security software which automatically detects and blocks fake websites. It also checks whether the major banking and shopping sites are original or not.

 

 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*