

Why Anti-Phishing?

In computing, phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message.

How is Phishing performed?

Most methods of phishing use some form of technical deception designed to make a link in an email appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers. An attacker will typically choose a bank, payment service or online auction site and target their customers. Like this example URL, <http://www.yourbank.com/> The next thing the attacker will do is to send mass mails to the user base of the chosen target site and inform the users that they need to login to their account and change their password because of a security risk or a system upgrade and they will provide a link to the fake site <http://www.yourbank.cm/> but in the email it will say <http://www.yourbank.com/> because the email is HTML then the user will then think the email is valid and visit the fake site and give their sensitive details. they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, although it is very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against PayPal.

What does Anti Phishing do or prevent?

The SecPoint Protector prevents Phishing using several techniques.

All emails are scanned for fake sites that do not match the content so if it not ok for just 1% the user gets a warning will be issued to the user. Other techniques are applied to block Phishing fake sites so that if a user by a mistake clicks a Phishing link it will be blocked anyway.

What can the user do to avoid getting scammed?

Tip #1: Do not click on links in your e-mail.

If you receive a message from your bank asking you to do something, do not click on links in the email and do not use forms in the email to log in. Instead, open your browser, go directly to your bank's website, log in, and continue there. Even if the email is from someone you know, DO NOT CLICK ON THE LINKS.

Tip #2: Invalid credentials usually work on impersonated websites.

If you feel there is something wrong with a website, use invalid username and invalid password to log in. If the website then presents you with the "Logon failed" page, you are *possibly* on a legitimate website. It may not always work as sometimes impersonators simulate failed logons for double-checking victim's input or redirect to a legitimate website after collecting credentials. But if your invalid credentials get you right through - it is definitely a phishing attempt.

Tip #3: Report the message to the company impersonated in the email.

Most financial organizations have guidelines and dedicated email addresses where to report security problems. If you suspect a message is a phishing attempt, forward it to the organization. You should include all email headers. Do not expect a reply from the organization as they receive thousands of those reports.