

AVG MULTI-LAYERED PHISHING PROTECTION

What is Phishing?

When Hackers try to trick you into providing the username and/or password to one of your accounts – that is called Phishing. These types of attacks used to require a talented developer to deliver, but can now be purchased inexpensively, in a kit form, complete with video instructions. They are inexpensive and require little technical skill to use, and so are now very common.

How can I spot a Phishing attempt?

It usually starts with an email from a seemingly trustworthy company saying that you need to login to your account to verify some information. The perpetrator of the Phishing attack will often try to create a sense of urgency by saying that your account has been, or will be, closed down unless you act. As in the real example below, there is usually a legitimate looking email address. And though it contains the word PayPal, it is actually not from PayPal (some email viewers will allow you to see the full address by right-clicking on it).

PayPal@ **important Notice : We Have Disabled Your Account Access** • Dear member

fig. 1: phishing email

When you click a link within the email to comply with their request – you are taken to a legitimate-looking website to enter your username and password. But in reality, the website is a fake and your login information is sent to the hacker instead.



fig. 2: flow of a phishing attack. . .

How does Phishing affect me?

Hackers will login with your password and then change it – to lock you out. They might read your email, post to your social media, order products, whatever the website allows. And, hackers know that people often use the same or similar usernames and passwords for many accounts, so they may try to use your login information on other popular websites. Hackers have software that makes it quick and easy to try out hundreds of variations of your username and password in just a few minutes.

What does AVG do to protect me?

AVG uses a multi-layered approach to provide you the best possible protection. First, we scan the web continuously to identify “Phishy” email and the websites they link to. Then we analyze those websites and also compare them with legitimate sites. If we determine that it is a Phishing site – we identify unique characteristics in the way it is coded – it’s like taking a fingerprint of the Phishing website. Those fingerprints are automatically loaded into your Virus Database, and now your AVG software can identify this Phishing site, and other sites that may use the same or similar code. Finally, AVG monitors links that you click and stops Phishing pages from loading and displays a message alerting you to the danger.

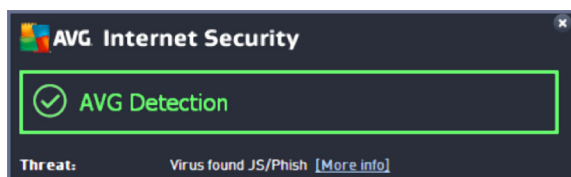


fig 3: detection message

What else can I do to avoid Phishing attacks?

- know that a reputable company will not reach out to you by email and ask you to login
- don’t open email or click links in email from unknown sources
- look at the senders full email address (any extra words or characters suggest it is a fake)
- don’t use the same password on multiple websites
- use passphrases (e.g. “20BlueBananas” instead of passwords)



AVG Multi-Layered Phishing Protection

AVG has 24/7, multi-layered, world-wide approach to protect you from Phishing. . .



- 1) Scour the web for “Phishy-Looking” Emails



- 2) Follow Email links to websites



- 3) Compare Phishy websites to legitimate sites



- 4) Fingerprint the Phishy site



- 5) Add Fingerprint to your AVG software



- 6) LinkScanner Prevents Phishy sites from loading



- 7) AVG displays warning