Types of phishing scams

The different forms of phishing that you need to be aware of

In generic terms, phishing is an online scam where a cybercriminal impersonates a trustworthy entity, such as company or brand, to obtain personal sensitive data from the victim. Some of the most impersonated brands include Microsoft, LinkedIn, Amazon, Google, PayPal and Zoom.

Phishing is nothing new and has been a practice used by cyber criminals for many years. However, what is worrying is the wide array of sophisticated methods being deployed to trap victims. Here we give an overview of the different types of phishing you need to be aware of.

Spear phishing

A more advanced phishing method whereby seemingly authentic phishing messages are targeted at specific groups, organisations or even individuals. Authors of spear phishing emails perform detailed research on their target(s) in advance, making it difficult to identify the content as fraudulent. Although often intended to steal data for fraudulent activity, cybercriminals may also intend to install malware on a target's computer or device.

Smishing

A form of phishing, smishing is when someone tries to trick you into giving them your private information via a text or SMS message. Smishing has now become an emerging and growing threat in the world of cyber security. This form of phishing is particularly alarming because people tend to be more inclined to trust a text message than an email.

Deceptive phishing

Deceptive phishing is the most common type of phishing scam. In this case, an email from a trusted company, such as a bank, asking you to click a link and verify your account details, is an example. The attacker attempts to obtain confidential information from the victims and then use it to steal money or to launch other attacks.

Whaling

This term has been phrased for when cybercriminals go after a "big fish" like a CEO or similar. These attackers often spend a considerable amount of time profiling the target to find the opportune moment and means of obtaining their credentials. High-level executives are able to access a great deal of company information, so whaling is of particular concern.

Pharming

Similar to phishing, pharming sends users to a fraudulent website that appears to be legitimate. However, in this case, victims do not even have to click a malicious link to be taken to the dishonest site. Attackers can infect either the user's computer or the website's DNS server and redirect the user to a false website even if the correct URL is typed in.

Contact us:
support@itg.uk.com
01625 613 633
www.itg.uk.com