**PHISHING :**

Phishing is the fraudulent attempt to obtain [sensitive information](https://en.wikipedia.org/wiki/Sensitive_information" \o "Sensitive information) or data, such as usernames, passwords and [credit card](https://en.wikipedia.org/wiki/Credit_card" \o "Credit card) details, by disguising oneself as a trustworthy entity in an [electronic communication](https://en.wikipedia.org/wiki/Electronic_communication" \o "Electronic communication).Typically carried out by [email spoofing](https://en.wikipedia.org/wiki/Email_spoofing" \o "Email spoofing),[[3]](https://en.wikipedia.org/wiki/Phishing" \l "cite_note-DMARC-3) [instant messaging](https://en.wikipedia.org/wiki/Instant_messaging" \o "Instant messaging), and text messaging, phishing often directs users to enter [personal information](https://en.wikipedia.org/wiki/Personal_information" \o "Personal information) at a fake website which matches the [look and feel](https://en.wikipedia.org/wiki/Look_and_feel" \o "Look and feel) of the legitimate site.

Phishing is an example of [social engineering](https://en.wikipedia.org/wiki/Social_engineering_(computer_security)" \o "Social engineering (computer security)) techniques used to deceive users.

Users are lured by communications purporting to be from trusted parties such as [social web sites](https://en.wikipedia.org/wiki/Social_networking_service" \o "Social networking service), [auction sites](https://en.wikipedia.org/wiki/Online_auction" \o "Online auction), banks, colleagues/executives, [online payment processors](https://en.wikipedia.org/wiki/E-commerce_payment_system" \o "E-commerce payment system) or IT administrators.

Attempts to deal with phishing incidents include [legislation](https://en.wikipedia.org/wiki/Legislation" \o "Legislation), user training, public awareness, and technical security measures (the latter being due to phishing attacks frequently exploiting weaknesses in current web security)

## **Types of Phishing :**

### **Spear phishing :**

Phishing attempts directed at specific individuals or companies is known as *spear phishing*. In contrast to bulk phishing, spear phishing attackers often gather and use personal information about their target to increase their probability of success.

The first study of social phishing, a type of spear phishing attack that leverages friendship information from social networks, yielded over 70 percent success rate in experiments.

**Whaling :**

The term whaling refers to spear phishing attacks directed specifically at senior executives and other high-profile targets. In these cases, the content will be crafted to target an upper manager and the person's role in the company. The content of a whaling attack email may be an executive issue such as a [subpoena](https://en.wikipedia.org/wiki/Subpoena" \o "Subpoena) or customer complaint.

### **Clone phishing :**

Clone phishing is a type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. T

### **Voice phishing :**

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts.

### **SMS phishing :**

SMS phishing or smishing uses [cell phone text messages](https://en.wikipedia.org/wiki/SMS" \o "SMS) to deliver the *bait* to induce people to divulge their personal information.. Smishing attacks typically invite the user to click a link, call a phone number, or contact an email address provided by the attacker via SMS message. The victim is then invited to provide their private data; often, credentials to other websites or services.