FIRESAND
END TO END SECURITY FOR YOUR BUSINESS

Office Address: Firesand Ltd,
Harben House, Suite B13, Severn Drive,
Newport Pagnell, Buckinghamshire,
MK16 9EY

Firesand's Top Tips

How to avoid Phishing Scams

Unlike viruses, worms and other malicious programs that attack your software and hardware, phishing scams attack YOU.
But there are ways you can protect yourself and your information.

Don't fall prey.

- **Use Firewalls – High-calibre** firewalls filter the **network traffic** that flows between you, your computer and outside users. This piece of **software blocks** unauthorised access from local and commercial networks, such as the **Internet.**

- **Be aware –** Look out for the **common signs** of a **phishing scam.** Whether that be an email that **does not address you directly** with both your first and/or last name, **or** an email that conveys an **overwhelming sense of urgency** whilst asking you for **personal information and/or sensitive data.** As legitimate **businesses will not do this.**

- **Think before you click –** Phishing scams often contain **deceptive links** that will have the **appearance of a legitimate URL address.** Do **NOT** click on these links. When in doubt, go to the website source directly.

Protect Yourself From Phishing.

T: 01908 477 588
M: 07720 850 434
E: info@firesand.co.uk
web www.firesand.co.uk

FIRESAND

END TO END SECURITY FOR YOUR BUSINESS

Common Phishing Scams include:

- **'The classic' email.** From Netflix, to government bodies like HMRC, many unauthorised users use these well-known, established and trusted companies because it is hard for us to ignore them.

- **Spear phishing**. Direct and calculated, these scams target specific individuals within an organisation. Using a blend of social engineering and phishing tactics to retrieve specific, personalized information.

- **SMiShing.** The same phishing tools and tactics used, but delivered via SMS text instead of email. Clicking on and downloading unsolicited content from a text message is just as damaging as a deceptive link from a suspicious email.

- **Domain squatting.** Used to add validity to phishing attacks. By registering a specific domain name to gain the trademarks that belong to that domain, unauthorised users give their scams an illusion of a legitimacy. These illusions/trademarks include inheriting the 'secure' padlock used by websites to show their authenticity.

Don't be complacent.

Report internet scams and phishing attacks when you see them and contact professional who can help ensure you are **secure**.