Avast Business

Avast partner educational series

Phishing & social engineering

16 September 2021

Avast Business

About the author

Rob Krug,
Senior Security Architect,
Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

It is typically carried out by email spoofing (faking the sender address) or instant messaging. It often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

Phishing is an example of social engineering techniques being used to deceive users.

What is Social Engineering?

Social engineering, in the context of information security, is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which doesn't concern the divulging of confidential information.

Social engineering differs from a traditional con in that it is often one of many steps in a very complex fraud scheme.

Generally speaking, social engineering has also been defined as any act that influences a person to take an action that may or may not be in their best interest.

Phishing Types

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.

Whaling
This type of attack 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.

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. The attachment or link within the email is replaced with a malicious version and sent from an email address spoofed to appear to come from the original sender.

Avast Business

Protection against Phishing / Social Engineering

User Training
People can be trained to recognize phishing attempts and to deal with them through a variety of approaches. Such education can be effective, especially when training emphasizes conceptual knowledge and provides direct feedback. Many organizations run regular, simulated phishing campaigns targeting their staff to measure effectiveness of their training.

Spam Filters
Spam filters detect malware-infected emails and prevent them from getting into inboxes. These filters can be applied to both inbound and outbound emails.

Website Checks/Alerts
It is helpful to have a technical security measure implemented that checks websites for legitimacy. If a spoof website is detected, then an alert will be triggered notifying the user.

Multi-Factor Authentication
Organizations can implement multi-factor authentication, which requires users to use at least two factors when logging in. For example, a user must first provide a password and a smart card when logging in to their account.

Email Content Redaction
This is a more extreme measure to take to protect against phishing and social engineering. Organizations that prioritize security over convenience can require users/office computers to use an email client that redacts URLs from email messages. Thus, making it impossible for the reader of an email to click on or copy a URL. This may result in an inconvenience, but it almost completely eliminates the threat of email phishing attacks. However, the reason phishing problems persist even after decades of anti-phishing software being sold is because phishing is actually a technological medium to exploit human weaknesses, and technology cannot fully compensate for human weaknesses.

About Avast Business

Avast delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit **www.avast.com/business**.