Guide

Decoding modern day

Phishing attacks

KNOWALL

PRIVATE CLOUD COMPUTING

Contents

Increasingly sophisticated

Since many companies have made the shift to remote working this has further increased the possibility of Phishing Attacks on company infrastructure. Many companies have had to quickly adapt to the new technologies and have not closed many secure gaps. This with the increase in personal and business devices is a major cause for concern as secure control is lost and no longer monitored.

According to Gov.uk 39% of UK companies have suffered security breaches or attacks in the last 12 months (Nov 1st 2021). These statistics indicates that hackers are focusing their efforts on spear-phishing and social engineering tactics to trick users into handing over their secure information. These attacks are becoming more and more sophisticated, and some would fool the most tech savvy of users.

Spear Phishing

Spear-phishing is when an attacker target a user and attempt to steal sensitive info such as login details or financial information from a specific user - often solely for malicious intent.

This happens by gathering personal details on the user such as their family & friends, address, company details, and what they have recently purchased online. The attackers then pose themselves as a trustworthy friend or person to acquire sensitive information, typically through an email or via some other online messaging platform. This type of attack roughly accounts for 90% of attacks that are trying to gain confidential information.

Social Engineering

Social engineering is a form of phishing attack that is used to manipulating users so they give up sensitive information. The types of details these cyber-criminals are looking for can vary, but when users are targeted the attackers are usually trying to fool the user into giving them your passwords or banking info, or access your computer to secretly install a malicious virus – this in turn will allow them full access to your PC and your passwords.

Attackers use social engineering tactics as it is generally easier to trick someone into giving over their details rather than trying to hack the password system themselves. Human manipulation and error is far easier.

39%

of UK businesses (4 in 10) have experienced cyber security breaches or attacks in the last 12 months (gov.uk)

1 in 5

UK businesses that have encountered an attack have ended up losing money, data or other assets (gov.uk)

46%

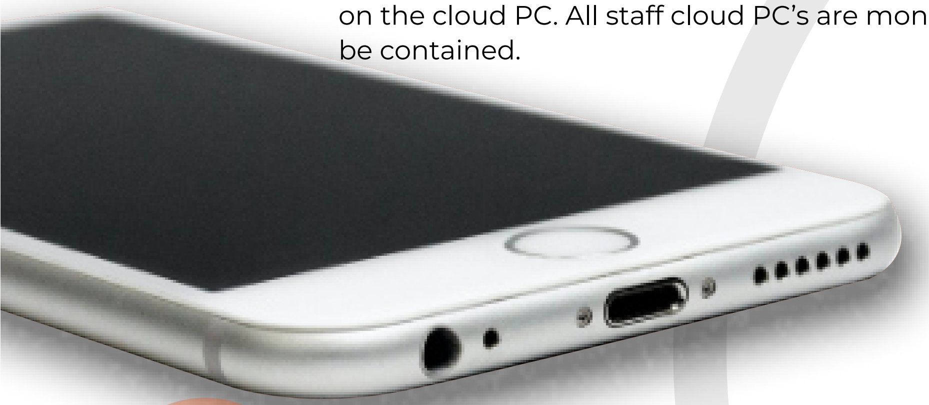
of businesses (Over four in ten) are using smart (i.e. network-connected) devices in workplaces (gov.uk)

Best Practices

1

Contain infrastructure with Azure

Azure is an incapsulated remote cloud service. Think of Azure as a remote PC that lives in the cloud. Staff will remotely login and access a cloud based PC where all apps and data will be held. No data will spill onto personal machines as its all held on the cloud PC. All staff cloud PC's are monitored for malicious activity and can be contained.



2

Multi-factor authentication with Duo

Multi-factor authentication (MFA) or two-factor authentication (2FA) are increasingly being made mandatory by organisations as they try to counteract the prevalence of phishing attacks and automated bot networks orchestrating credential stuffing attacks.

A key example of how effective 2FA is – In 2017 Google made it mandatory that all of its employees use 2FA security methods and issued nearly all of its employees with USB-based 2FA keys. Out of the 85,000 employees at the time, none had fallen victim to a phishing attack due to the effectiveness of 2FA.

3

Endpoint Detection and Response protection with Carbon Black

Endpoint Detection and Response (EDR) is a fully managed service supplying expert professionals, technology and industry intelligence needed to hunt, lockdown and remediate attacks. By continuously monitoring your organisations endpoints and conducting detailed forensics, our expert Cyber Security Operations Centre (CSOC) professionals obtain a real-time awareness of attackers' movements in order to enhance threat discovery capabilities.

4

Run a real life phishing simulations

Run a real life phishing simulation within your company to spot the staff that might need better guidance. And equip your staff with the right knowledge and tools to spot phishing scams quickly.

The threat of cyber-attacks continues to grow globally and the methods employed by hackers are becoming more sophisticated. We advise all of our clients to consider extra measures to mitigate the risk of IT systems being compromised.

KNOWALL
PRIVATE CLOUD COMPUTING

Security Solutions that Deliver Business Protection

Helping you safeguard your business from modern day threats

Get in touch

020 7471 3270 / sales@knowall.net

knowall.net