wavex
EXPERIENCE EXCELLENCE

How to survive a

PHISHING ATTACK

Summary

With the growing volume of automated and focused cyber-crime attacks, no business is safe with over 45% of UK businesses having already fallen victim of phishing attacks in past 2 years.

The consequences of infection can range from benign, as your systems act as a carrier, or fatal, if systems are seriously compromised and good backups do not exist.

As more businesses move to cloud solutions for their email, phishing emails can easily propagate without a virus ever infecting your PC – the hacker can do it all remotely by scanning all your contacts and emails, then sending the phishing attack to your colleagues and clients.

Key FACTS

£3.03m
The average financial cost of a data breach

90%
For phishing accounts of data breaches

15%
of people successfully phished will be targeted at least one more time within the year

76%
of businesses reported being a victim of a phishing attack in the last year

You've been hit. So, what do you do?

Here are some best practices you can follow to minimise the damage caused by a phishing attack

Stay CALM

Unfortunately, you are in good company when it comes to being a subject of a phishing scam. However, in the immediate aftermath of the incident you can make the issue better (or far worse). Keeping a cool head is important.
Do not delete anything as this will be helpful later in determining exactly what has occurred.

Minimise the spread of INFECTION

If you have provided your username/password to an online service, it is unlikely this step will help.

However, if you have inadvertently run or downloaded something to your computer, this step could be helpful.

You can remove your computer from the network (disconnect the RJ-45 cable from the back).

If you are using WiFi you should put it into airplane mode. On Windows 10 this is done via the Start Menu/Settings/vNetwork.

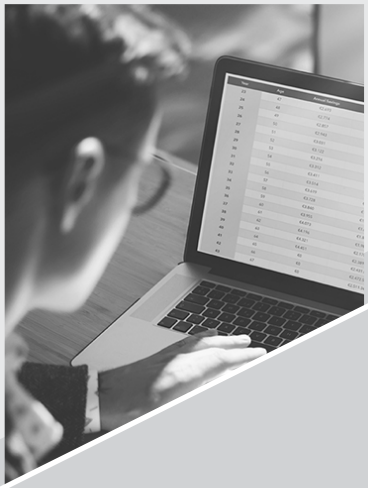
However, because many businesses now have email servers in the Cloud, for instance Office 365, if you have accidently provided your Microsoft Office 365 credentials the attack can occur without any access to your computer so removal from the network will have little impact.

Important - You also need to notify your IT function that your computer is no longer on the network otherwise once they have removed the virus you will inevitably reconnect your computer and the infection will start again.

Also, by removing your computer you will find it impossible to perform the following steps, so it is very dependent upon what has actually occurred.

Check email
FORWARDING RULES

Many attacks first establish an email forwarding rule, so any new emails are automatically sent on to the hacker. It is important any unfamiliar forwarding rules are removed otherwise despite resetting your password the hacker will still receive copies of your emails.



Reset your
PASSWORD

The current advice is to use a combination of words although it is likely your system will have its own complexity requirements. Most providers use 2 factor authentications for password changes. In other words, they will send you an SMS containing a code which is used in the password changing process.

Notify your
STAKEHOLDERS

IT DEPARTMENT

Alert your IT function of what has happened. The more information you provide them the better they can determine exactly what has happened.

They will help assess the impact and how much data may have been stolen.

If you do not have an IT department then the following activities should be performed

- Scan your computer(s) and laptop(s) for viruses
- You can use a website like https://www.hybrid-analysis.com/ to find out more about the attack. This may help you determine your level of exposure.

CLIENTS

If the breach is likely to adversely impact the personal or privacy of your clients, you need to tell them the following:

- Your name and contact details
- The estimated date of the breach
- A summary of the incident
- The nature and content of the personal data
- The likely effect on the individual
- Any measures you have taken to address the breach
- How they can mitigate any possible adverse impact

Information Commissioner's Office (ICO)

If PII (personal identifiable information) has been taken, you will need to notify the ICO within 24 hours of becoming aware of the essential facts of the breach. You should include the following information

- Your name and contact details
- The date and time of the breach (or an estimate)
- The date and time you detected it
- Basic information about the type of breach
- Basic information about the personal data concerned

Remain VIGILANT

If you have revealed any financial information you should watch for signs of identity theft or financial transactions. If you are confident financial information has been taken you should contact the associated banks to ensure the information taken cannot be exploited.

Minimise your FUTURE RISKS

Unfortunately, understanding what vulnerabilities exist is not simple and often expensive.

The old-style solutions with virus scanners on your PCs and a firewall on your Internet connection can no longer protect companies from sophisticated attacks which are mostly performed indiscriminately across large numbers of companies, since it only takes one person within your organisation to open the "front door" to hackers.

With all businesses facing this threat, vulnerability detection has to be a core part of any IT service proposition.

The top 5 critical reasons for this are:

FREQUENCY

When a vulnerability is found, hackers often extract information about your IT setup, which is then distributed, making you a regular target for other types of attack. It is far better to avoid the first one.

SOPHISTICATION

Cyber-crime is increasing in regularity and sophistication. Businesses should act now to get in front of the trend.

REPUTATION

Due to the way all viruses spread, any breach is unlikely to remain a private matter. Often email address books are queried in order to send the infection to your clients and partners.

RISKS

If you do not know your vulnerabilities you have no way of protecting yourself.

COST

Recovering from cyber-crime can be expensive in terms of IT cost, lost-productivity and data loss.

> There are a range of other proactive measures you can take depending on your organisation

Implement a cyber response process – This is similar to a fire-drill where the actions to follow ing/during a cyber incident are understood across the business. This helps minimise mistakes and provides the means for the organ isation to improve its sophistication when addressing threats.

Technology adoption – There is a lot of technology designed to minimise risks. The one that will have the largest positive impact is multi-factor authentication (MFA or 2FA). This involves an additional step when accessing online resources and makes it impossible for a hacker to access your data even if they have obtained your username and password. In addition to this, there are a range of email filtering applications that also help to reduce the volume of phishing emails.

About the AUTHOR

Gavin Russell is the CEO & founder of Wavex Technology Limited, a London based managed IT services provider and Microsoft Gold partner. Having spent over 30 years in the IT industry Gavin started his career as a software developer then moved to an IT infrastructure role in AT&T, responsible for IT operations across EMEA.

After gaining experience of how large businesses manage technology, he decided to form Wavex with a focus on delivering the best possible end-user experience when it comes to IT support, security and cloud for small to mid-sized businesses.

Wavex has now been going for 20 years, has won countless awards, and supports many thousands of users, counting amongst them are a number of prestigious company's. Despite his CEO responsibilities, Gavin continues to maintain close working relationships with the executives of his clients; helping them to solve a range of challenges and use technology to realise their business goals.

https://www.linkedin.com/in/gavinrussell1/

Multiple Awards Winner

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2018

intY FINALIST Expert Partner of the Year 2018

intY FINALIST Azure Partner of the Year 2018

SHORTLISTED IT SERVICE & SUPPORT AWARDS 2019 BEST SMALL EMSP 2019

IT EUROPA EUROPEAN IT & SOFTWARE EXCELLENCE AWARDS 2019 FINALIST

Affiliations & Certifications

Microsoft Partner Gold Cloud Platform
Microsoft Partner Gold Cloud Productivity
Microsoft Partner Gold Datacenter

CYBER ESSENTIALS PLUS

Microsoft Partner Silver Application Development
Microsoft Partner Silver Small and Midmarket Cloud Solutions
Microsoft Partner Silver Collaboration and Content