Don’t Take the Bait

Defending the Third Sector Against Scams

Identity Experts

Microsoft Partner
Microsoft

Gold Security
Gold Cloud Platform
Gold Data Analytics
Gold Windows and Devices

Scammers Are Filling Their Nets

At a time when data is perhaps more valuable than oil, organisations are facing some of the biggest threats of their existence in the form of scams – particularly ‘phishing’ and ‘smishing’.

The former, you may be familiar with, but the latter continues to be an evasive enemy for many organisations to pin down. The result is a workforce who aren’t equipped to detect and respond to scams – leaving data open to theft and leaks.

Although a data breach is a dangerous challenge for any organisation, those inhabiting space in the Third Sector easily find themselves at even more of a disadvantage.

Did you know?

Phishing accounts for 90% of data breaches

With vulnerable people in their care, limited resources, and the interest of hackers putting targets on their back, Third Sector organisations must do more to defend their data, protect their staff, and safeguard vulnerable people.

Furthermore, the measuring of GDPR compliance by the CQC has placed an extra regulatory burden on organisations such as hospices, care homes, and medical facilities.

Before you panic, however, we’re here to help. In this document, you’ll find some practical advice to help curb the threat posed by phishing and smishing scams. Got any questions? You’ll find our contact details on the last page.

Phishing
A fraudulent communication that seems genuine to the recipient – but which seeks to do harm.

Smishing
Specifically a fraudulent text message that seems genuine to the recipient – but which seeks to do harm.

How to Defend Your Team

As an organisation, you have a duty of care towards your employees and volunteers – and defending against scams starts with defending your team. The following advice will start you off on the right track to safeguard data and arm your team with the knowledge, skills, and resources they need to stay safe.

Education is Key
Action starts with education; train your team on the importance of staying vigilant, how to spot a scam, and how to react.

Use [Lookout/MS]
There are tools at your disposal – such as [SOLUTION].

Encourage Action
Let teams know that caution is more important than being right.

Create a BYOD Policy
Close any gaps in your security perimeter without jeopardising remote working.

Run a Test
Put your team to the test with a faux scam and see who takes the bait.

Everybody is a Priority
From the chairperson to the volunteers, every third sector worker is crucial to the success of this initiative – nobody should be left behind.

What Kind of Solutions Am I Looking For?
Password etc.

How Users Can Defend Themselves

No matter the tools at your disposal, a lot of staying secure rests in the hands of responsible users.

Phishing and smishing scams aren't only aimed at organisations, with individuals finding themselves in crosshairs, both in their personal and professional lives.

In most cases, you'll be protected by the expertise of your IT team, or by the specialist technology that forms your security perimeter. Regardless of this protection, however, some of the responsibility still falls to you, the user.

Fortunately, there are some simple steps you can take to play your role and stay safe.

Does it Look Right?

Is the wording unusual? Is it a request you'd usually field? Is the tone correct?

Verify it's True

If in doubt about a request that involves sharing data or sending money, pick up the phone and ask.

Check Credentials

Ensure a website has the correct, up to date certificate before inputting details. Is the URL correct and recognisable?

Don't Gamble

Still not sure? Adopt a Zero Trust approach: never trust, always verify.

What Else Can I Do?

In addition to the above, remember to follow your IT team's lead on staying safe, and abide by the rule of never giving away a password or any other valuable details over the phone or by email.

How to Protect the Vulnerable

Through their incredible work with individuals, causes, and communities, organisations in the third sector have the opportunity to engage with vulnerable people – and to pass on insights to keep them safe.

The following is advice that can be passed onto individuals and groups to ensure that they're not taking the bait from phishing attacks.

Does it Look Right?

Is the wording unusual? Is it a request you'd usually field? Is the tone correct?

Verify it's True

If in doubt about a request that involves sharing data or sending money, pick up the phone and ask.

Define Communications

Detail your organisation's approved communication methods, as well as limits on what details they'll be asked to share.

Check Credentials

Ensure a website has the correct, up to date certificate before inputting details. Is the URL correct and recognisable?

Secure Tools

Provide them with secure solutions and tools.

Don't Gamble

Still not sure? Adopt a Zero Trust approach: never trust, always verify.

Further text

Where to Begin

Ask for Help

A lot of organisations are facing the same threats – there's nothing to be embarrassed about.

Alert Your People

Education is the cornerstone of preventing phishing attacks – so gather your people for a briefing.

Seek Solutions

The onus can't be entirely on your organisation's people: seek out the right tools to keep them safe.

Did you know?

1 in 25 branded emails are phishing scams

The phishing threat may feel at first overwhelming, and might

Before you panic, however, we're here to help. In this document, you'll find some practical advice to help curb the threat posed by phishing and smishing scams. Got any questions? You'll find our contact details on the last page.

About Us

Identity Experts is a distinguished, UK-based Microsoft Gold Partner, focused on identity access management (IAM) and security.

Since 2014, our passionate team of experts has worked alongside organisations to provide a holistic approach to their technological needs, backed by experience and ever-expanding knowledge, and our partner relationships.

Together, we help to ensure our customers' security, create savings on resources such as time and cost, and underpin further organisational transformation.

With direct links into Microsoft's product engineering teams, we're able to provide best-in-class implementation services, influence product roadmaps, and represent Microsoft Consulting Services and the Microsoft FastTrack team.

How Can We Help?

Secure Organisations

Manage Identities

Support Transformation

Upskill Teams

Identity Experts

Microsoft Partner
Microsoft

Gold Security
Gold Cloud Platform
Gold Data Analytics
Gold Windows and Devices

Tel: 03333 444950 | **Email:** info@identityexperts.co.uk | **Twitter:** @identityexperts