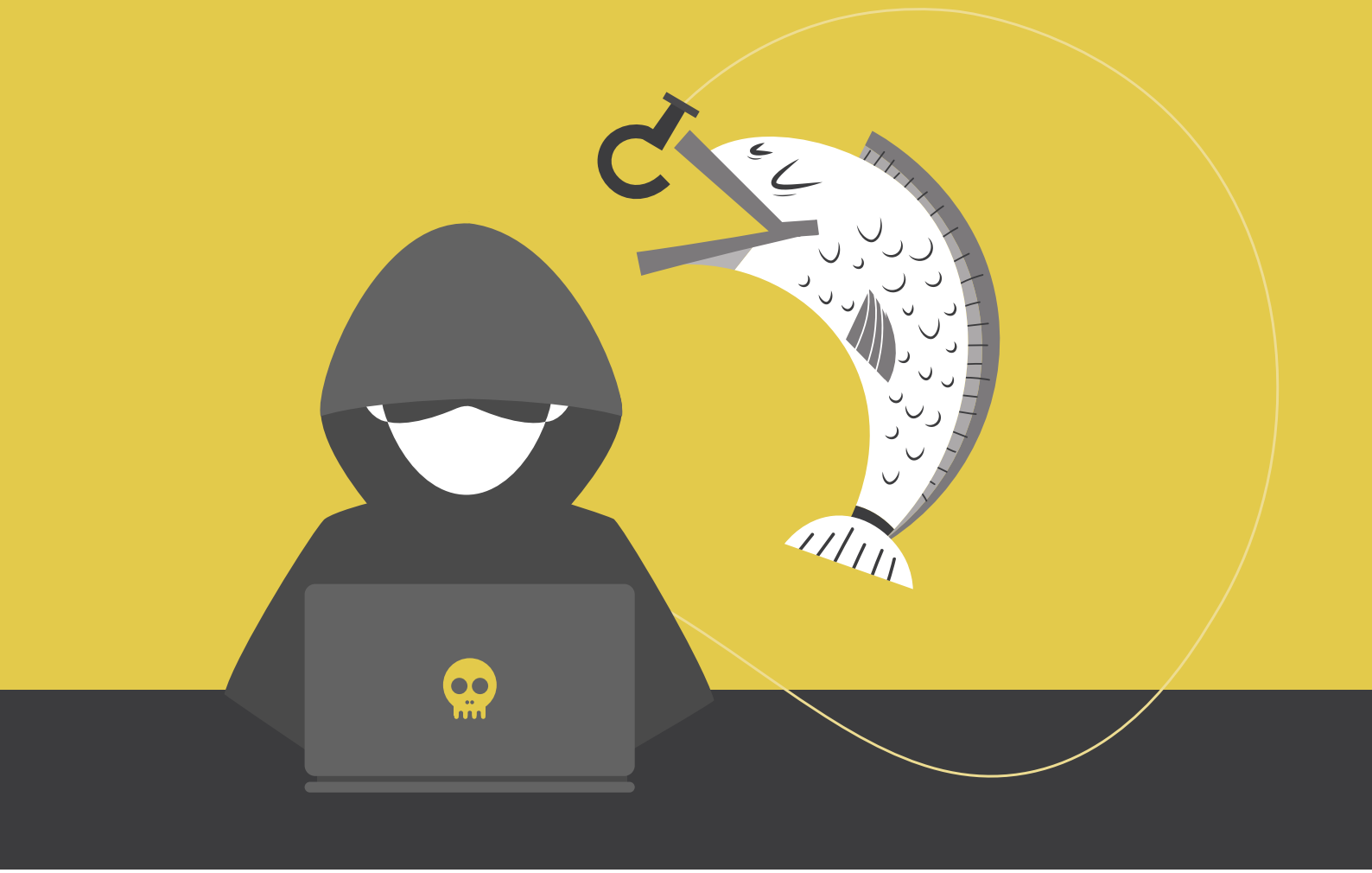
Phishing:

Don’t be easy bait!



Phishing:
Don’t be easy bait!

We’d like to start with a little story.

Cast your mind back just a few weeks to that long, blisteringly hot summer. It’s a balmy evening and Trevor the trout is happily swimming along in the lake, minding his own business. He’s a simple soul is Trevor, and he likes nothing more than meandering along among the rocks and algae, just taking it all in.

He’s heard tales of scary humans who sit by the water with big sticks, luring fish like him away from their families, but he’s never actually seen one himself. Besides, he’s careful. He wouldn’t get caught out like the other silly fish. “I’ll be fine” he says to himself. “Nobody’s going to pick on me.”

Out of nowhere, something above the water catches his eye. It’s the biggest, juiciest insect he’s ever seen in his life. It smells deliciously revolting, and he can’t resist it. He leaps towards the surface, catches it in his mouth and closes his eyes, ready to savour this fine delicacy.

Uh-oh. Before he has any time to think, poor Trevor’s flying through the air towards what he quickly realises must be one of those legendary scary humans.

He’s caught on a hook, and no matter how hard he tries he can’t get free.

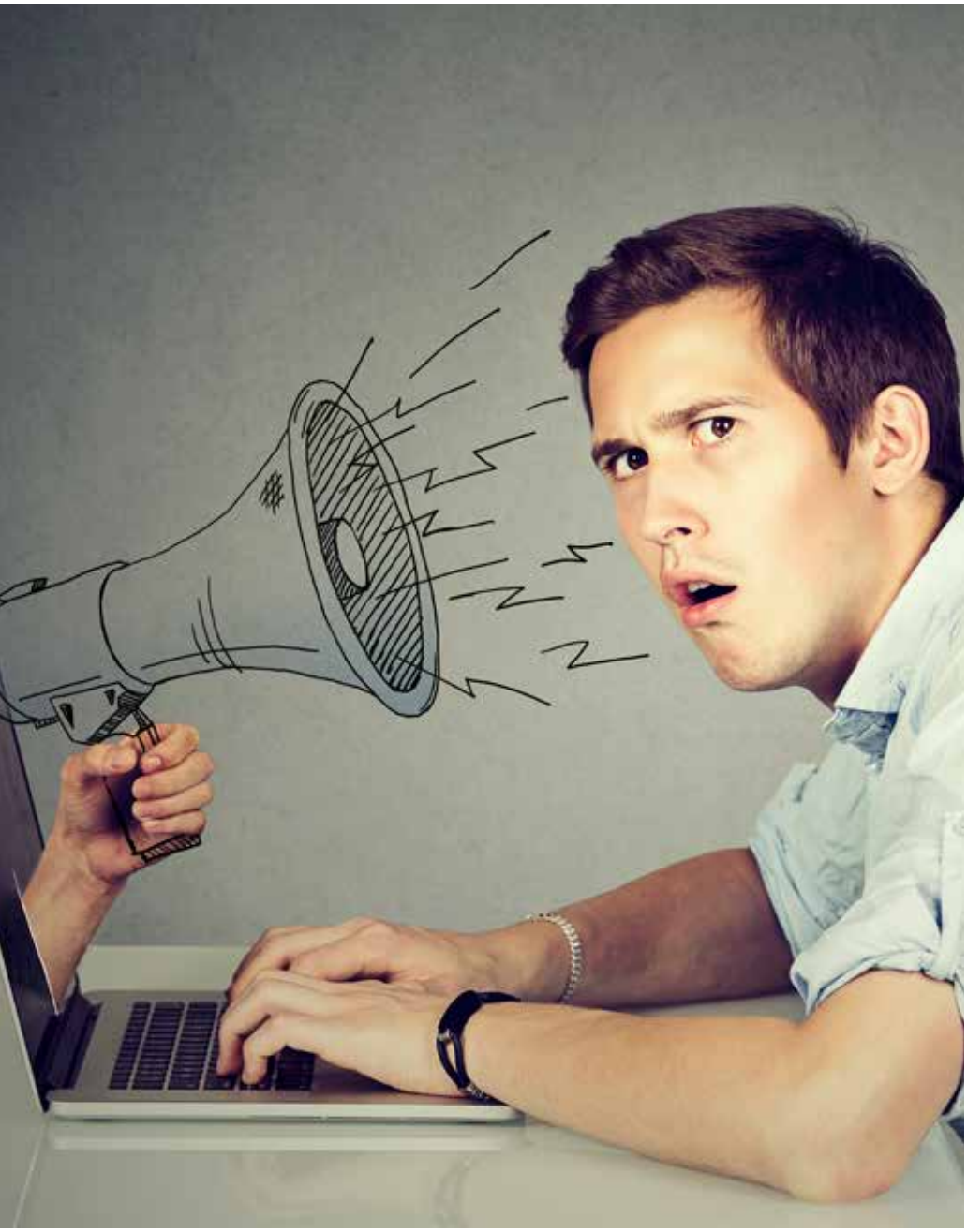
Within a few short minutes it’s all over, and later that same evening he’s someone else’s dinner.

The end.

Not exactly War and Peace, and we’re sorry if Trevor’s sad tale has put you off your tea. But we’re here to tell you all about phishing, and it’s got a lot more in common with the popular leisure activity than name alone.

What is phishing?

Cyber crime is big business, and phishing attacks are one of the baddies' favourite routes into an organisation. You've probably heard of them, but you might not be 100% clear on exactly what they are and how they work. Here's a simple definition:



A phishing scam happens when a cybercriminal pretends to be someone else to gain information. Commonly they do this by sending fake emails designed to look like they're from a trusted source, such as the Chief Executive or Head of Accounts.

The aim is to make the victim feel a sense of fear, curiosity or urgency so they quickly open a dodgy attachment, or send important details like bank/credit card details, user names or passwords.

They rely on the fact that most staff are eager to please their superiors and won't question them, so they freely give out sensitive information they would normally hang on to.

If you're thinking only an idiot could get caught out by such a blatant scam, you might be surprised

These people are very skilled at what they do and can create emails that look so much like the real thing that even the savviest staff member can easily be caught out at the end of a busy day.

For that very reason, phishing scams are often deployed towards 5pm or last thing on a Friday when people just want to get home and take their eyes off the ball.

Just like the fisherman sitting patiently at the riverside, hackers know that if they wait long enough, someone will bite sooner or later.

Some more statistics you need to know

£1.22 million

The average cost of a phishing attack for a mid-sized company is £1.22 million. That sort of money is difficult for any company to give up, but for many it could signal the end altogether.

65%

Phishing attempts rose by 65% between 2017 and 2018. They're not specific to any particular industry and businesses of all sizes have been attacked.

30%

30% of phishing messages are opened by targeted users, with 12% of those users going on to click the links or attachments.

1.5

Nearly 1.5 new phishing sites are created every month.

Back to the fishing analogy for a moment

There are lots of different ways to catch a fish. Paddling in rockpools with a net; rod fishing; line fishing; trawling; spear fishing and more. Phishing takes different forms too, and to have any chance of staying ahead of the cyber criminals you need to understand how they will try to reel you in.

A recent Gmail phishing scam targeted nearly a billion users across the globe. It was fiendishly simple but tricked a lot of people.

Here's how it worked.

Victims received a text message asking if they'd requested a new password for their Gmail accounts. Of course, the vast majority had not.

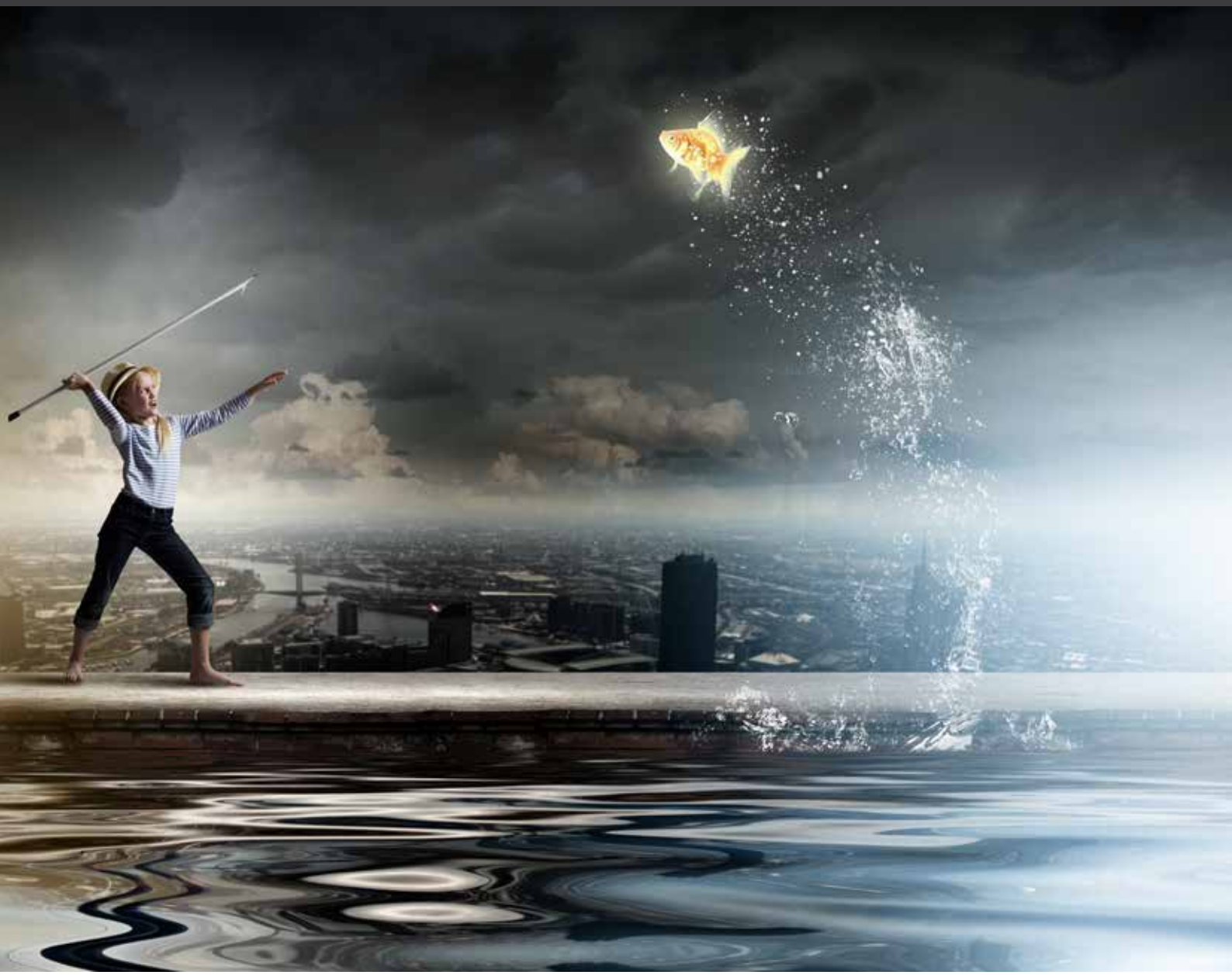
Confused targets were then prompted to text back "STOP" to confirm the request had nothing to do with them. They were then sent another text urging them to send their 6-digit numerical access code to prevent their accounts being compromised.

Of course, the opposite was really happening. Instead of protecting their Gmail accounts, they were giving the hackers the ability to reset their passwords. And so, access to all their emails.

This type of phishing scam is known as a "wide net attack".

Trawlers cast wide nets to catch a huge amount of fish and seafood that won't all be good enough to sell, and this method uses the same principle. You can't expect 100% success, but plenty will fall for it. And in this case, even a relatively small catch can reap impressive rewards.

The other type of phishing attack is more targeted, and it's known as **"spear fishing"**



In this case, hackers know exactly who they're looking for and will focus all their efforts on these unsuspecting victims. Because this isn't a blanket approach the hackers have to be more creative and thoughtful in their hunt. It's common for them to use carefully chosen phrases and tailor their language to suit each individual person or group.

In a lot of cases spear phishing attacks are so convincing that they're able to completely fool the target into parting with all sorts of information, blissfully unaware that they've been caught out.

You might still be reading this thinking **"It'll never happen to me"**

Maybe it won't. But can you be as confident about every single one of your staff workers and business contacts? Plenty of intelligent people have taken the bait, which is exactly how the scammers keep going.

There are ways to avoid falling prey to phishing attacks. Here are a few top tips:

Stay informed:
Education is everything, and that goes for you and your staff members. New scams are being developed every day, so it pays to sign up to regular updates and guides that will keep you in the loop. Cyber Security training for all IT users is also highly recommended so you can be confident that everyone knows what to look out for.

Be suspicious:
OK, so it's a bit miserable going through life being cynical but there are some situations where it pays to expect the worst. If an email doesn't look quite right, it probably isn't. If you're not sure, just hover over the link before clicking on it to see where it leads to. If you don't recognise the website address or it's full of funny looking symbols, avoid like the plague. A lot of phishing emails start with "dear customer" so be particularly wary of any that don't address you by name. And if there are lots of grammatical errors and language that sounds very old fashioned, it's almost always going to be from a scammer.

Get protection:
Install anti-virus protection, SPAM filters, web filters and anti-phishing toolbars and make sure they're always kept up to date. Failure to install the latest patches and updates leaves organisations wide open to threats. Monitor the anti-virus status of all equipment, particularly mobile devices that are used outside of the working environment.

Think ahead:
Develop a robust IT security policy that includes everything from Bring Your Own Device to password management and backups. Make sure all sensitive company information is encrypted and that all mobile devices – including those that belong to staff members – have to pass security protocols before they can access your network.

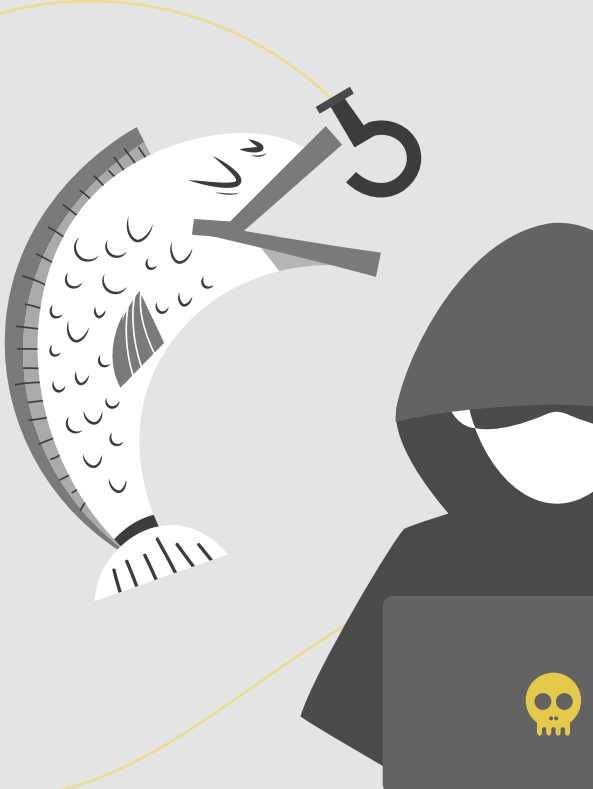
Check regularly:
Check all your online accounts at least once a month. If you haven't used an online account for a few months it could already have fallen foul to hackers. Change your passwords regularly, thoroughly check all your messages and transactions, and if you don't use them at all, close them down.

Keep your technology up-to-date:
Keep your web browser up to date. It might seem like a pain having to keep installing new patches on your internet browser, but updates are there for a reason. Providers release patches in response to phishing attacks and loopholes, so don't ignore messages to update.

Block pop-ups:
A lot of hackers will try to infiltrate your system by deploying bright and colourful pop-up boxes. If one does sneak through, never click the "cancel" button – go to the "x" at the upper right instead.

Keep it private:
Never share personal information over the internet unless you're 100% certain you can trust who you're talking to and you're sure your data is encrypted. If a company ever asks you to impart sensitive information, check with them at source first by visiting their main website and calling the customer services team.

Don't be a trout:
Don't be tempted by precious or shiny things. We humans aren't so very different to poor Trevor the Trout. The promise of a precious prize has caught out many an internet user, like that big juicy insect dangling above the water. If you receive a message in your inbox telling you you've won a competition you don't remember entering, step away.



The best way to keep the phishermen away?

Put your IT security in the hands of some trusted professionals.

You're already working hard, so you could probably do without the hassle of having to keep your entire computer system ship shape and safe from cyber attackers.

Working in partnership with reputable IT experts who can prove they're worth their salt will help you sleep better at night and send the hackers further upstream to in search of a better catch.

We'd love to do a security audit on your business and uncover the technology and people areas where you are at risk.

Contact us today