Want to learn the tricks of a master manipulator?

Read on...

How Does Cybercrime Work?

The Art of Manipulation

We reveal the tricks cybercriminals use to outwit their victims.

No-one can manipulate me... can they?

We all have a weak spot, and it's decision-making. Not the big decisions (although they're tricky enough!) but the little ones. How to sit, where to look, whether to have another sip of coffee.

To make all these decisions, we need to use unconscious rules of thumb. We gain a lot of time this way, but we also create room for error.

Cybercriminals send emails that try to trigger our unconscious rules of thumb. They know that if we act consciously on a phishing email, we're less likely to fall for it.

What do I need to watch out for?

Cybercriminals use lots of tactics to push us into quick decision-making.

An attachment with an intriguing title might make us too curious to resist. The danger of missing out—only one left!—can push us to act without thinking, as can a tight deadline.

Other tactics trigger our social instincts. A phishing email might seem to come from an authority figure, like your boss, or from someone who seems a lot like you. In fact, we're likely to trust people who say they know us, even if we don't recognise them! Some emails rely on our habit of following our peers: "80% of your colleagues have already completed the survey."

Our newsletter series will be looking at the TOP 3 main tactics: Curiosity; Authority and Scarcity

Watch out for the first instalment, on curiosity manipulation.

Top 3 Tactics

01 Emails that seem to come from an authority figure

02 Scarcity: "Act now or lose out!"

03 Incomplete information that makes us curious

If you spot signs that an email is trying to manipulate you, carefully review its contents. If you're suspicious, report it at once to your manager or a member of the IT / Security team.

Look out

for our new training lessons on the 7 persuasion techniques and how to identify them in phishing

You won't believe what she's seeing...

Curious?
Read on...

2

How Does Cybercrime Work?

Manipulating Curiosity

Learn how cybercriminals hack human curiosity to catch out their victims.

What is Curiosity, Really?

Have you ever seen a child rip open a toy 'blind bag,' only to instantly discard the toy? Even as an adult, you might check the news before you've had your morning coffee.

Curiosity is powerful. It's an urge to seek out new information. It's sometimes so strong that we rush to find something out, and delays can make us impatient or anxious.

We develop curiosity from an early age, because it's extremely useful. The urge to find out more helps us learn, innovate, take on new challenges, and enjoy our hobbies.

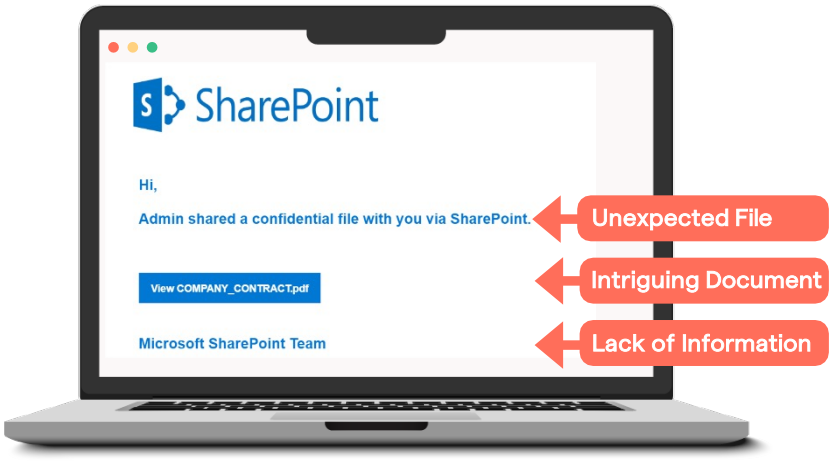
But curiosity can also be used against us.

How Do Cybercriminals Exploit Curiosity?

Cybercriminals exploit the human need to scratch a mental itch. If you saw a mysterious QRI code in an unlikely place, would you be tempted to scan it? It could be a trap set by a cyber-manipulator.

Phishing emails use tricks as simple as an interesting headline that invites you to "click to read on," or an attachment with a curious title. Most of us won't fall for it most of the time, but if enough people receive it, some will click before their rational brain can interrupt that curious urge.

Protect yourself by learning the tell-tale signs of curiosity manipulation. Take a look at our handy primer:



The Takeaways

Watch out for:

01 Solitary links

02 'Learn more'

03 Unexpected files, folders or parcels

If you spot signs that an email is trying to make you curious, carefully review its contents. If you're suspicious, report it at once to your manager or a member of the IT / Security team.

Look out

for our new training lessons on the 7 persuasion techniques and how to identify them in phishing

You heard Uncle Sam.

Better read on...

3 How Does Cybercrime Work?

The Authority Principle

Learn how cybercriminals use our respect for authority to catch us out.

What is Authority, Really?

OK: Uncle Sam isn't going to make you read an email. But what if your boss told you to? Would you even check what it was before you opened it?

We learn to obey authority from the moment we're born. Following the rules set by our parents and teachers keeps us safe and helps us to become good members of the community.

By the time we're adults, obeying authority has become a deep-seated habit.

That means it can be used against us.

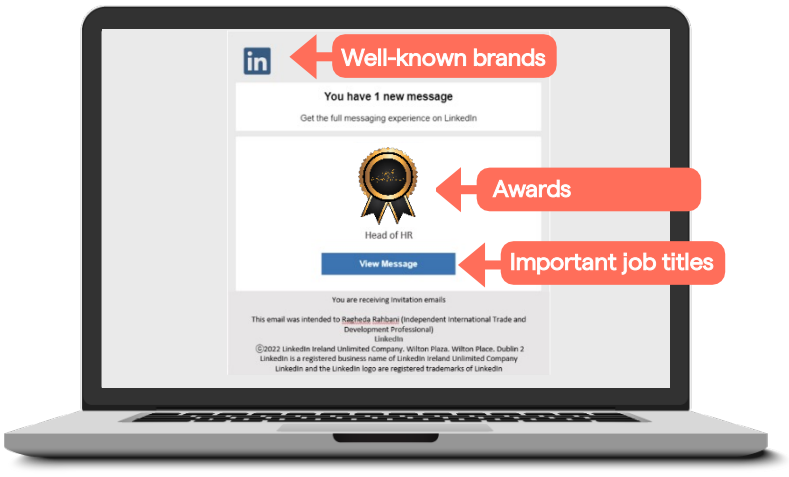
How Do Cybercriminals Exploit Authority?

Cybercriminals know we'll often act without thinking when we believe we're obeying someone in authority.

That's why phishing emails often appear to come from well-known brands, government bodies, or people with important job titles, like CEO. Awards and accreditations can also give an email the appearance of authority.

Because we're in the habit of responding to authority, some of us will act on these signs before our rational minds have a chance to stop us.

Protect yourself by learning the tell-tale signs of authority manipulation. Take a look at our handy primer:



The Takeaways

Watch out for:

01 Job titles

02 Brands and government bodies

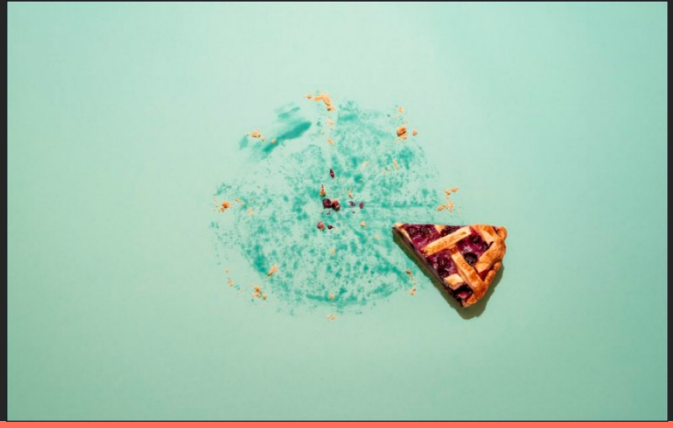
03 Awards and accreditations

If you spot signs that an email is using the authority principle, carefully review its contents. If you're suspicious, report it at once to your manager or a member of the IT / Security team.

Look out

for our new training lessons on the 7 persuasion techniques and how to identify them in phishing

Last chance to get your slice!



Tempted?

Read on...

4

How Does Cybercrime Work?

The Scarcity Principle

Learn how cybercriminals manipulate our anxiety about things (and time) running out

What is Scarcity?

Have you ever seen people queueing round the block to buy a limited edition? Maybe you've done it yourself!

When something seems rare or hard to get, we automatically feel that it's more valuable. This is an in-built human bias. Deep down, what we really value is freedom of choice. It's not that we necessarily want the limited edition: we just don't want to lose the option of having it. When resources are scarce, it's a sensible survival strategy.

But the fact that it's an automatic response means it can be used against us.

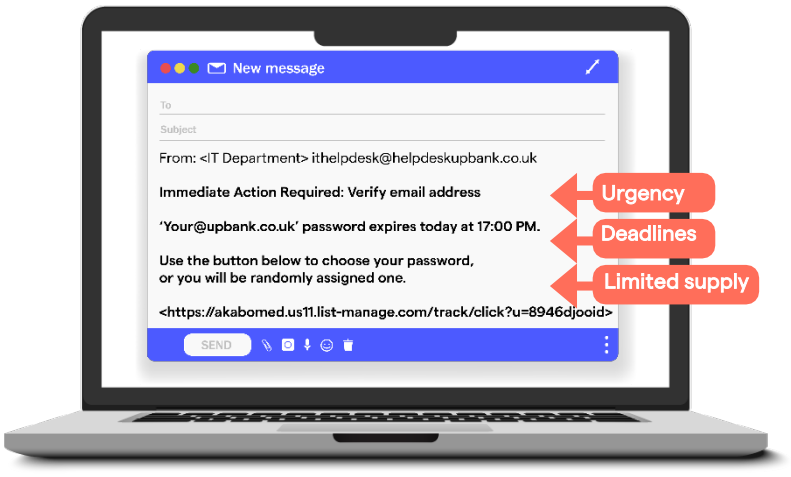
How Do Cybercriminals Exploit Scarcity?

Cybercriminals know we'll often act impulsively when something seems scarce. They can make us even more impulsive by setting a time limit for action.

That's why phishing emails often urge you to act quickly, either to gain something or to avoid a loss. These emails might make a tempting offer that expires today, or warn you that you'll lose access to an account unless you respond within 24 hours.

Because of our natural scarcity bias, some of us will act on these signs before our rational minds have a chance to stop us.

Protect yourself by learning the tell-tale signs of scarcity manipulation. Take a look at our handy primer:



The Takeaways

Watch out for:

01 Urgency

02 Deadlines

03 Limitations

If you spot signs that an email is using the scarcity principle, carefully review its contents. If you're suspicious, report it at once to your manager or a member of the IT / Security team.

Look out

for our new training lessons on the 7 persuasion techniques and how to identify them in phishing