

The real story behind social engineering

Making misconceptions a thing of the past

The more you know about your people, their vulnerabilities and privileges, and those wishing to cause them harm, the better you can keep social engineering attacks at bay. But as we get better at identifying potential threats, cybercriminals evolve their methods and behave in ways you may not expect.

To help you stay one step ahead, here are the latest trends, behaviours and common misconceptions about threat actors and their methods of attack.

Misconception #1

Threat actors prefer hit and run attacks

The reality:

Cybercriminals often spend time researching and building rapport before execution.



TA453

TA453, an Iranian-aligned group, frequently use benign conversation in their campaigns in order to solicit information from targets.

TA406

North Korea's TA406 attempts to collect victims' credentials and other information before sending malicious links or attachments.

TA499

TA499, a Russia-aligned threat actor, sent seemingly harmless emails to solicit information from high-profile individuals prior to launching its attacks.

Misconception #2

Legitimate services such as Google and Microsoft are safe to use

The reality:

Threat actors regularly abuse legitimate services to harvest credentials, and host and distribute malware.



14%

14% of all observed malicious campaigns leveraged legitimate services.

G

Google-related URLs were the most frequently abused...

Microsoft

But Microsoft-related URLs earned more than twice the clicks of those hosted by Google.

Misconception #3

Threat actors only use email

The reality:

Proofpoint's industry-leading threat intelligence identified increased attacks leveraging call center-based email threats.



250K

Proofpoint observed over 250,000 telephone-oriented (TOAD) attacks every day.

Headset

TOAD emails don't contain links or attachments. They require victims to proactively call a fake call center.

\$50K

In one case, a victim lost almost \$50,000 to a TOAD attack.

Misconception #4

Internal conversation threads are always safe

The reality:

Thread or conversation hijacking is a popular technique with a number of high-volume, financially motivated attackers.



x500

Proofpoint observed over 500 campaigns using thread hijacking

x16

...distributing 16 different families of malware...

Malware icons

...including Qbot, Emotet, IcedID and Raccoon Stealer.

Misconception #5

Threat actors only use standardised, business-related content

The reality:

Cybercriminals capitalise on current events, news, popular culture, and much more to encourage engagement with malicious content.



Network icon

In 2021, Proofpoint observed hundreds of millions of COVID-themed lures every month.

Document icon

Tax themes are a regular favourite of cybercriminals – offering rebates in exchange for a variety of sensitive information.

Triangle icon

Other observed lures include... Valentine's Day Squid Game Ukraine/Russia war Support for refugees

Find out more



Download Proofpoint's Social Engineering Report

Additional resources

READ THE BLOG [Icon]

Discover last year's strangest social engineering tactics in this blog post by Proofpoint's threat researchers.

LISTEN TO THE PODCAST [Icon]

Social Engineering: How Threat Actors Manipulate Their Targets. In this podcast, Proofpoint explains how bad actors capitalise on our humanity to attack us.

GET IN TOUCH [Icon]

Book a meeting with Proofpoint to find out how we can protect your organisation. Ask us about our free risk assessments.

For more information, visit proofpoint.com

PROTECT PEOPLE. DEFEND DATA.

Attackers know that the easiest way into your organisation is through your users. Defend them. Protect them. Empower them with Proofpoint. Every day we protect the people at more Fortune 500 and Global 2000 organisations than anyone else.

We analyse... 2.6B+ email messages | 49B+ URLs | 1.9B+ attachments | 28.2M+ cloud accounts | 1.7B+ mobile messages | ...Every day