whitepaper

when 'legitimate' becomes the weapon

the age of obvious phishing is behind us.

gone are the poorly written emails, suspicious links, and fake login pages that once raised red flags for users. today's cyber threats are more polished, more believable and, unfortunately, more effective.

among the most sophisticated is the adversary-in-the-middle (AitM) attack. unlike traditional phishing, AitM doesn't rely on tricking users into giving up their passwords. it takes things a step further, silently hijacking entire sessions in real time, even with multi-factor authentication (MFA) in place.

here's how it works, and what you can do to stay ahead.

the new face of phishing

picture this scenario:

you receive a Dropbox notification

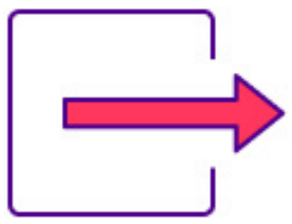
- **from a trusted colleague,**
  with a subject line like “Mohammed Isa shared invoice 2059 with you”

- **sharing a document**
  as they normally would

- **looks completely authentic**

you click the malicious link

- land on the "**real**" Dropbox login
- **perfect** branding and design
- the security certificate is **valid**



you login and complete MFA

behind the scenes, an attacker has just gained access to your session, and **everything** that comes with it.

find out what makes AitM different

what makes AitM different

traditional phishing	AitM attacks
creates fake login pages to steal passwords	uses a proxy to insert themselves between you and the real service

here's what makes them so dangerous:

real-time interception

rather than creating fake login pages, attackers relay your login attempt to the actual service while simultaneously capturing your credentials and session tokens.

complete session hijacking

they don't just steal your password, they also inherit your entire authenticated session, including all the permissions and access that come with it.

MFA bypass

because the attacker is relaying your authentication in real-time to the legitimate service, even multi-factor authentication provides no protection.

in essence: when you log in, they log in with you.

quick security glossary

- [ ] **multi-factor authentication (MFA)**
  additional login security requiring multiple verification methods beyond just passwords.

- [ ] **adversary-in-the-middle (AitM)**
  advanced phishing using reverse proxies to hijack real-time login sessions.

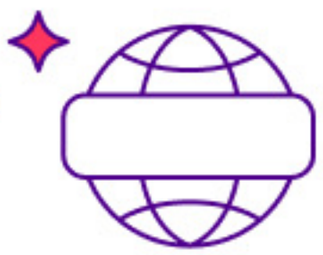
- [ ] **phishing**
  deceptive messages that trick users into revealing sensitive information by impersonating trusted sources.

- [ ] **cybersecurity**
  protecting systems, networks, and data from digital threats to keep operations running.

- [ ] **proxy**
  an intermediary server/device that routes traffic between a user and another server/device.

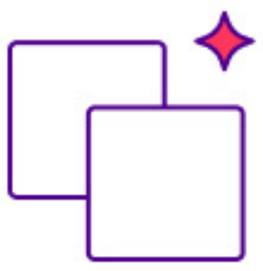
why these attacks succeed where other fail

- **AitM attacks are devastatingly effective because they eliminate the traditional red flags that users are trained to spot:**



no suspicious domains

the attack may use subdomains of legitimate services or sophisticated lookalikes that pass casual inspection



perfect visual replication

since they're proxying the real login page, the appearance is flawless

bypasses email filters

many attacks leverage compromised legitimate accounts or trusted platforms, making them invisible to traditional security tools

legitimate SSL certificates

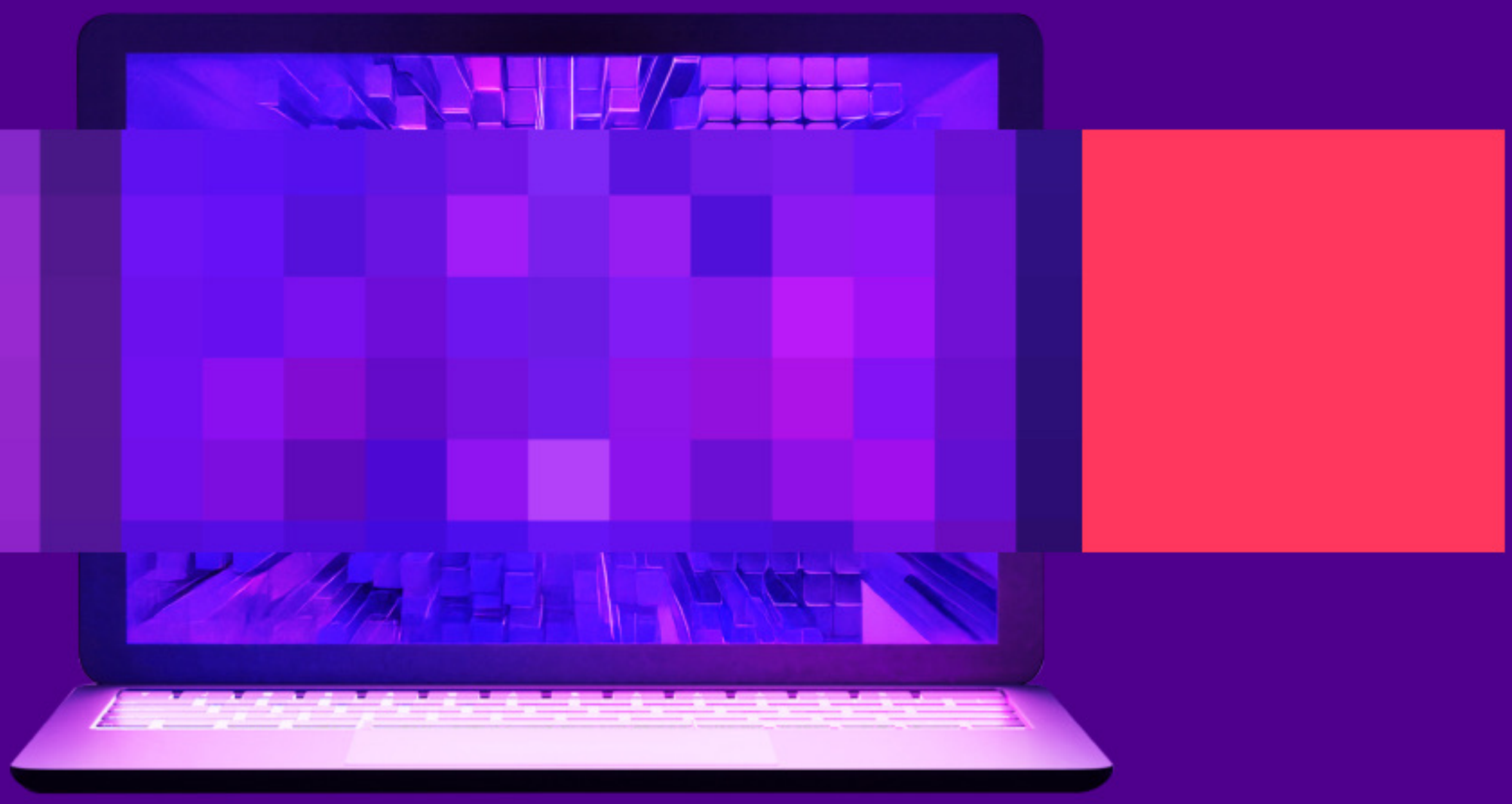
the connection appears secure because, in many ways, it is

from the user's perspective, **nothing feels out of place, which is exactly why it works.**

who is most at risk

AitM attacks are increasingly used in high-value, targeted phishing campaigns. **typical targets include**:

1. IT and security admins with elevated access
2. HR and operations staff managing employee data and approvals
3. executive teams and finance leaders with access to sensitive systems
4. remote and hybrid workers logging in from various devices and networks



these groups are often seen as high-impact entry points into the wider organisation. however, the scope of attacks is broad, with lower priority groups still a target.

the misconception that MFA provides complete protection makes these attacks even more dangerous. organisations often have a false sense of security, believing they're immune to credential-based attacks.

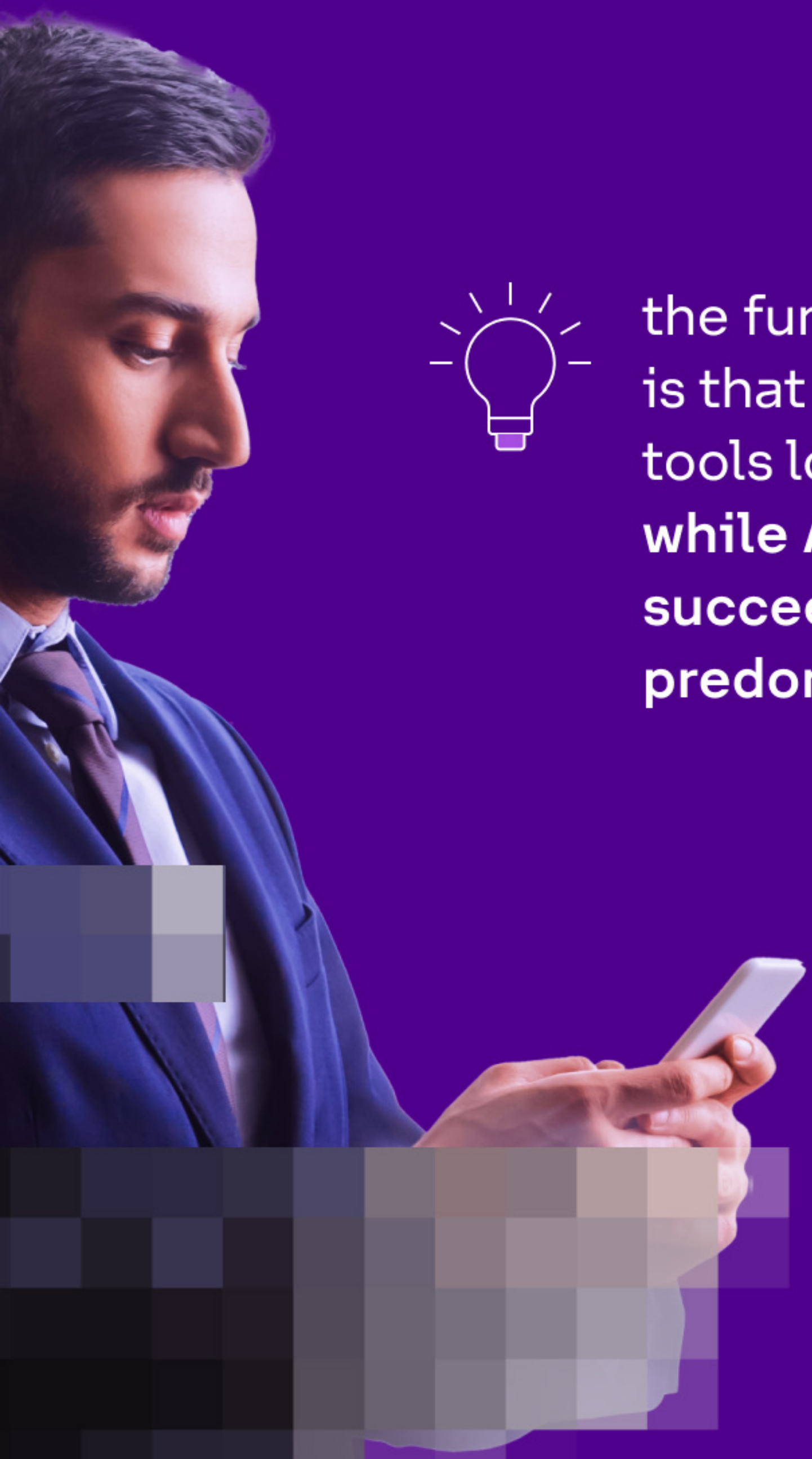
the limitations of traditional security

most cybersecurity tools are designed to detect known threats

- flagged domains
- suspicious attachments
- anomalous login attempts

but AitM attacks operate differently

- they use legitimate and trusted services and infrastructure
- they behave like real users
- they generate activity that blends in with everyday operations



the fundamental problem is that traditional security tools look for what's fake, **while AitM attacks succeed by being predominantly real.**

why behavioural detection matters

at stc bahrain, we take a different approach. we focus on how your business actually behaves rather than just what an attack looks like.

our network detection & response (NDR) solution, powered by Darktrace, uses ai-driven behavioural analytics to identify deviations in real time.

it doesn’t just scan for signatures. it learns your organisation's patterns, so even when everything looks normal, subtle anomalies stand out.

this includes:

- unusual login behaviour
  (e.g. simultaneous logins from two locations)
- suspicious post-login activity
  (e.g. registering new security information or setting up a new Microsoft authenticator)
- unexpected access flows and communication changes

when looking legitimate is the attack

AitM is part of a broader shift in cyber threats, one where the most dangerous attacks don't look dangerous at all.

when phishing links look perfect, and authentication flows behave exactly as expected, traditional defences may not be enough. what's needed is visibility into the subtle deviations that betray an attacker's presence.

success in that environment requires:

continuous behavioural monitoring

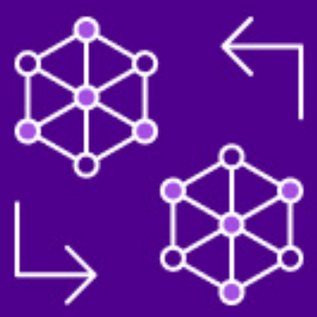
that understands what normal looks like for your organisation

real-time threat detection

that can identify subtle anomalies in user and system behaviour

contextual analysis

that considers the full picture of user activity, not just individual events



proactive response capabilities

that can contain threats before they spread throughout your environment

building resilience

- cyber threats are changing.
  but so are the tools to fight them.
- with stc bahrain, you
  can move beyond static
  protection and into
  proactive defence.
- we help you gain the
  visibility and intelligence
  needed to detect threats
  that others miss.
- because when looking
  legitimate becomes the
  threat, behavioral context
  makes all the difference.

contact us today to learn how we can **protect your organisation from sophisticated cyber threats.**