# The attacks you never saw:

## Real attacks our security team has stopped

ramsac
the secure choice

Most cyber attacks start with a stolen login, and many leave no visible sign. Here's how our 24/7 cybersecurity monitoring and response solution spots them, and recent success stories.

### How it works

1. **We watch.** Our tools monitor sign-ins, email, devices and systems around the clock for anything unusual.
2. **We investigate.** Our cybersecurity team checks each alert to find out what's really going on.
3. **We act.** We lock accounts, end attackers' sessions and block their addresses before damage is done.

### Now it's minutes

A year ago, attackers often waited days or weeks before using a stolen login. Now it's automated, and within minutes they can forward your emails, message your contacts and download your files.

**Why catching it early matters: With one stolen login, attackers can redirect payments, steal confidential files or email clients as you. Catching it early stops an alert becoming financial loss, leaked data or a breach you must explain to clients, insurers or to the Information Commissioner's Office (ICO)**

## Recent success stories

### A fake SharePoint link

**What happened**

In the kind of attack we see most often, a user received what looked like an everyday SharePoint file share. The link led to a fake login page, where they entered their password and MFA code. The attacker passed both on to Microsoft and captured the signed-in session, an adversary-in-the-middle attack that gets round MFA completely.

**What was at risk**

The attacker could now use SharePoint as that user, and the user had no idea anything had gone wrong.

**What we did**

Our monitoring saw the account signed in from two different places at once and raised a high-severity alert. Our team locked the account and cleared every active session before any data was taken.

### A leaked password and one tap of "approve"

**What happened**

A user's password had been exposed in a data breach at another organisation. An attacker tried it on their Microsoft account, and when an MFA request popped up on the user's phone, they approved it, assuming it was their own sign-in.

**What was at risk**

With the password and the approval, the attacker had everything they needed to get into the account and the data behind it.

**What we did**

Our monitoring spotted the sign-in from an unfamiliar internet address and locked the account automatically, before any data was accessed. Our team then reset the password and suggested some refresher security awareness training.

## A message from a friend

**What happened**

An employee got an email in their personal inbox from a friend whose account had been hacked. The link opened a login page, and they entered their work email address and password.

**What was at risk**

The attacker was now inside the business account. They registered a device of their own so they could get back in later, started reading emails and tried to use the account to attack others. No spam filter or antivirus could have stopped this, because it began outside the business altogether.

**What we did**

Our monitoring flagged the activity quickly, and our team locked the account before the attacker got any further.

## A laptop stolen from a car

**What happened**

A laptop holding sensitive data was stolen from an employee's car.

**What was at risk**

Anyone who could read the drive would have the data on it, and possibly a way into the employee's accounts. Losing a device that holds personal data may also need reporting to the ICO.

**What we did**

We confirmed the drive was encrypted with BitLocker, so its contents couldn't be read, sent a command to wipe it remotely and set up monitoring for any attempt to connect it. Our team also kept a close eye on the employee's account. No data was compromised.

## The email they were expecting

**What happened**

A client met a new contact at a conference and was expecting their follow-up email. It arrived from the right person at the right time, but the sender's account had already been hacked, and the attacker had slipped a malicious link into the draft. Our client clicked it.

**What was at risk**

Their own account was now compromised, and there was nothing they could have spotted. The only defence was noticing the activity that followed.

**What we did**

Our monitoring picked up suspicious activity on the account, including a sign-in from an unfamiliar device using a VPN service it hadn't been seen on before. Our systems revoked the account's access token to shut the attacker out, and our team started looking into how they'd got in.

## A flood of MFA prompts

**What happened**

A user's password was stolen in a phishing attack. The attacker then sent request after request to their phone, hoping they'd approve one just to make it stop. The user kept declining.

**What was at risk**

Declining was right, but the attacker still had a working password. Without monitoring, nobody would have known to change it.

**What we did**

Our monitoring picked up the declined requests and alerted our team, who blocked the attacker's internet address, reset the password and showed the user how to spot this kind of attack next time.

## Attempts to break into a firewall

**What happened**

An attacker tried to guess the login for the firewall protecting a client's office network, working through combinations one after another in what's known as a brute-force attack.

**What was at risk**

The firewall is the front door to the office network. Anyone who got into it could change its settings and open a way in to everything behind it.

**What we did**

We spotted the attempts, blocked the attacker's internet address and helped the client restrict the firewall's management console to approved addresses, closing that route to future attackers.

## Checking up on an account

**What happened**

An organisation had concerns about one employee and asked us for a record of everything that person did on their systems over the following week.

**What was at risk**

Without clear evidence, they'd have been making a sensitive decision about a member of staff on suspicion alone, which is unfair on the employee and risky for the business.

**What we did**

We used our security tools to capture the activity and worked through it with them, showing exactly which documents had been opened, so they could decide what to do next based on the facts.

## A free game on a home computer

**What happened**

An employee downloaded a free game onto their home computer, and hidden inside was malware that stole everything saved in the browser. That included a session token for their work email, the digital pass that keeps you signed in without re-entering your password or multi-factor authentication (MFA) code.

**What was at risk**

The attacker used the token straight away. With monitoring of account activity, the business would have no idea.

**What we did**

Our monitoring flagged the account being used from a device we didn't recognise, connecting through a new VPN service. Because the attacker was relying on the stolen session token, our systems cancelled it, cutting off their access, and our team then investigated how the token had been taken.



**Your Technology. Our Responsibility**

Want to find out more about our cybersecurity monitoring and response solution?

Call us on 01483 412 040 or visit www.ramsac.com

ramsac
the secure choice