Seven new (and convincing!) phishing scams

Learn the signs you need to watch out for

egress

Inside the report

Introduction

Cybersecurity would be much simpler if criminal groups would stick to the same old tried and tested methods. Sadly, that's never going to happen – they're persistent and creative. Instead, cybersecurity teams need to keep up to date with the latest tricks in the criminal playbook.

There's no standing still when it comes to cybercrime. Just as the neatest garden will eventually be overrun with weeds without a vigilant gardener watching over it, better cybersecurity defences are constantly needed when new phishing attacks pop up. And so the arms race goes on…

It's important that non-experts stay well-acquainted with phishing tactics too – after all, they're the ones the scammers are trying to target. So, here are seven emerging phishing trends we're seeing that you need to be aware of. We'll also cover how to keep yourself and your colleagues safe from these attacks (as well as future ones!).

Just as the neatest garden will eventually be overrun with weeds without a vigilant gardener watching over it, better cybersecurity defences are constantly needed

The scams

1 Supercharged spoofing

Spoofing is nothing new – it's where a scammer creates a fake display name, email address, or website to trick someone. They can look believable at first glance, but are often intercepted by email authentication tools. Now attackers are upping their game to get around traditional defences.

We've seen impersonations of well-known and trusted brands such as YouTube, Netflix, LinkedIn and Zoom. Even more sinister are the impersonation attempts of people you actually know. You might be surprised how well a good hacker can mimic the communication style and mannerisms of a CEO after studying their social media posts and blogs or videos available on corporate websites.

We're seeing new attempts to develop spoofed emails that escape the clutches of authentication tools. They do leave certain traces of the technology used to create them – but this is near impossible to spot with the human eye. Only intelligent tech powered by AI can pick up on the tell-tale signs.

You might be surprised how well a hacker can mimic the communication style of a CEO

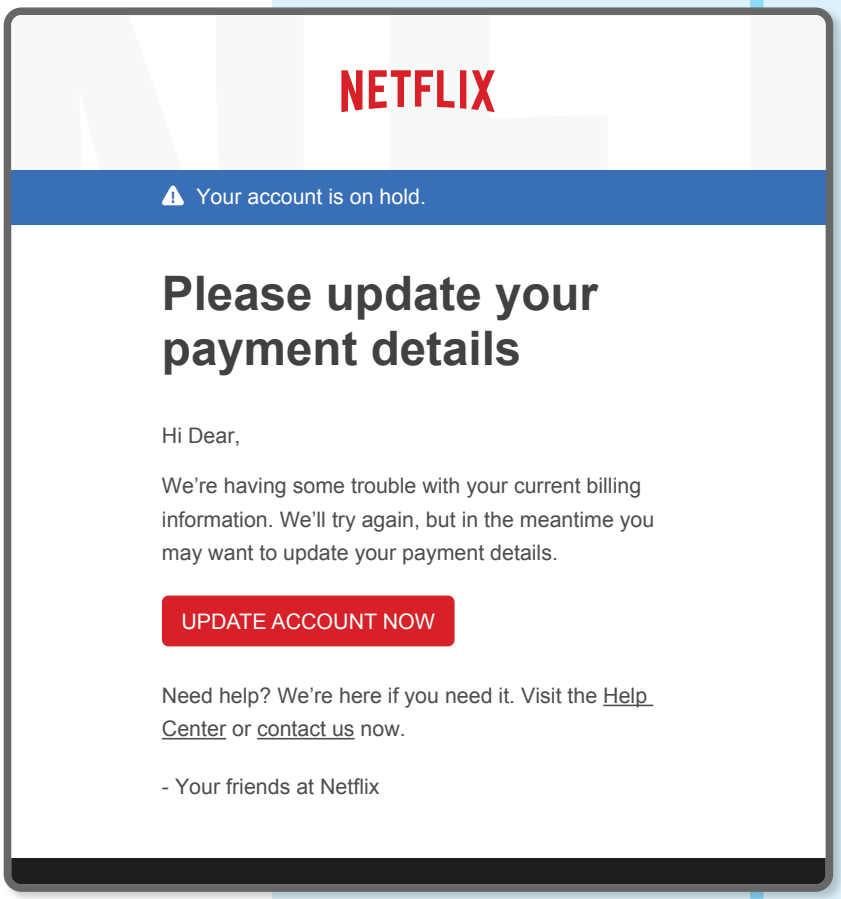


Image source: Federal Trade Commission Consumer Information

2 Deepfake it ‘til you make it

The next generation of phishing attacks is around the corner. Deepfake technology has been around for a while, but we expect it to become a bigger phishing problem in the coming years. In a nutshell, a deepfake is a piece of video or audio content that has been manipulated with AI. As you can imagine, the possibilities for online mischief are near endless.

Impersonation attacks via email can already be pretty convincing. Cybercriminals trawl social media to make these emails highly believable, picking up on sign-offs, signatures, chains of command, communication style, and even quirks of phrase. Adding a deepfake of a voice message or even a video call would take impersonation attempts to the next level of convincing.

Consider a high-profile case from 2019. AI was used to mimic the voice of a German conglomerate’s CEO and trick an employee at another business into transferring funds to the wrong bank account. Cybercriminals managed to steal almost $250,000 from a UK-based energy company with the scam. The victim said it sounded just like the CEO, even down to his slight German accent.

Deepfakes sound complicated, but they’re surprisingly easy for non-experts to make. The tech is legal to purchase, readily available, and will only get better. It’s likely the only way to stop deepfakes will be to fight fire with fire: AI recognition.

Deepfakes sound complicated, but they’re surprisingly easy for non-experts to make

3 Morse code. Yep... morse code!

When we said hackers get creative, we meant it. They don't just look for cutting-edge technology, but anything that can give them the edge over defences. And sometimes that means turning to older techniques. In this case, Morse code, which is something you might associate more with a World War I movie.

Since July 2020, Microsoft 365 users have been targeted with fake Excel documents that include JavaScript files used to steal passwords. Once opened, a dialogue box appears asking for login details – which are promptly harvested and stored by the hackers. According to Microsoft research, they changed their obfuscation and encryption mechanisms every 37 days during this scam.

However this one tactic in particular caught the eye of the cybersecurity community – during February and May of this year, the links to the JavaScript files were encoded using ASCII, then into Morse code to keep them hidden from detection software.

Morse code uses combinations of dashes and pulses to encode the 26 letters of the alphabet. The famous example for SOS being: '. . . - - - . . .'. Hackers took the base elements of Morse code and made it more complex to include numbers too, helping the malicious script to slip past traditional secure email gateways. Here's an example of what it looks like:

Invoice_1308._xslx.hTML

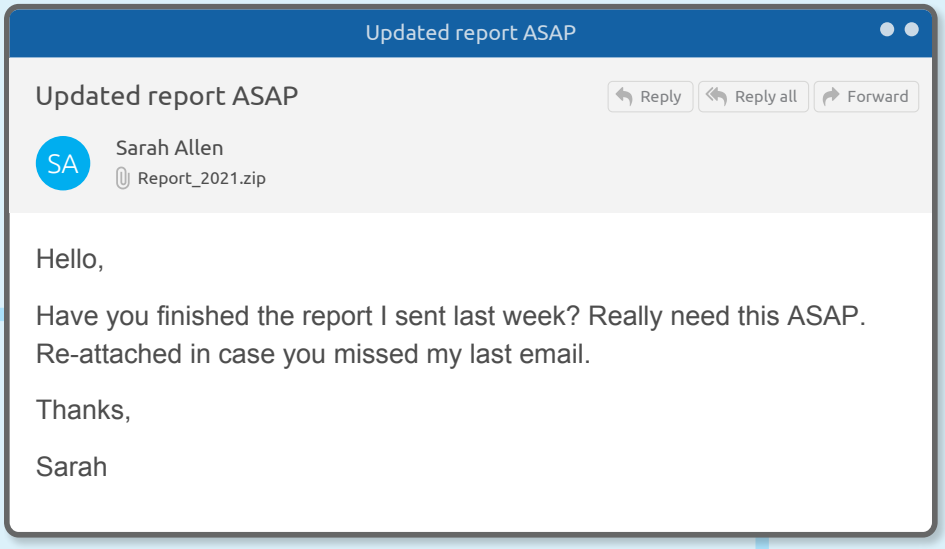
```
<!doctype html>
<html>
<body>

<p id="message"></p>

<script>
function decodeMorse(morseCode) {
        var ref = {
        '.-': 'a','-...': 'b','-.-.': 'c','-..': 'd','.': 'e','..-.': 'f','--.': 'g',
'....': 'h','..': 'i','.---': 'j','-.-': 'k','.-..': 'l','--': 'm','-.': 'n','---': 'o',
'.--.': 'p','--.-': 'q','.-.': 'r','...': 's','-': 't','..-': 'u','...-': 'v','.--': 'w',
'-..-': 'x','-.--': 'y','--..': 'z','.----': '1','..---': '2','...--': '3','....-': '4','.....': '5',
'-....': '6','--...': '7','---..': '8','----.': '9','-----': '0',
};

return morseCode
        .split('   ')
        .map(
          a => a
            .split(' ')
            .map(
              b => ref[b]
            ).join('')
        ).join(' ');
}

var decoded = decodeMorse("- .... .. ...  .--. .... .. ... .... .. -. --.  . -- .- .. .-..  -.-. --- -.
- .- .. -. ...  -- --- .-. ... .  -.-. --- -.. .  .-- .... .. -.-. ....  .. ...  ..- ... . -..  -... .-..  .... .-
-.-. -.- . .-. ...  - ---  .- ...- --- .. -..  -.-. .-.. -... . .-. ... . -.-. ..- .-. .. - .-..  ... --- ..-. - .--
.- .-. . .-.-.-  - .... .. ...  .--. .... .. ... .... .. -. --.  . -- .- .. .-..  -.-. --- -. - .- .. -. ...  -- ---
.-. ... .  -.-. --- -.. .  .-- .... .. -.-. ....  .. ...  ..- ... . -..  -... .-..  .... .- -.-. -.- . .-. ...  - ---
 .- ...- --- .. -..  -.-. .-.. -... . .-. ... . -.-. ..- .-. .. - .-..  ... --- ..-. - .-- .- .-. . .-.-.-  - .... ..
```

Image source: Bleeping Computer

4 Don't annoy the 'boss'. Missed message phishing

This sneaky tactic relies on first compromising the email account of someone within the business – preferably a senior executive. Attackers will often use a targeted spear phishing attack to get hold of an individual's login credentials. From there, they can take over the email account. The key danger with account takeover is that the attacker now controls a legitimate mailbox within your business, so any further malicious emails won't be picked up by traditional technology.

Attackers pressure the victim into reacting quickly, thinking they've annoyed their boss by missing some work



Once an executive's account is compromised, the attacker sends a junior colleague over a piece of completed 'work', such as a report. Of course, it's actually malware. With almost everyone on LinkedIn these days, it's not rocket science for hackers to work out the chains of command within a business. It's even better for the attacker if the targeted employee is a recent joiner.

The clever part is they'll mention that this piece of fake work was 'missed' in a previous, fictional email. This pressures the victim into reacting quickly, as they think they've annoyed their boss by missing something. Urgency is key in phishing, as the longer we think about the email and its request, the more likely our cybersecurity training will kick in and we will spot the signs of something not being quite right.

Remember to take a second to think when opening attachments (even if your boss does sound grumpy).

5 Hiding in plain sight (or site)

Criminals are now exploiting vulnerabilities to create malicious (but real!) pages on well-known brand sites. Because the link is genuinely going to a page on the brand's site, it's impossible to tell whether the link is malicious. This is exactly what happened with the recent UPS case.

A phishing campaign exploited a vulnerability on ups.com that looked extremely realistic. All the links in the phishing emails were legitimate, except for the tracking number. When victims clicked it, they were taken to the actual UPS website. From there, a malicious JavaScript injection made the page display a message letting users know a file was going to be downloaded. It was (of course) malware.

What makes this phishing method particularly concerning, is the fact that attackers can run an automated scan of hundreds of thousands websites at once to detect these vulnerabilities. This gives them a ready-made list of websites that can be easily compromised.

The attackers will either go after these sites themselves, or make the most of the 'Crime-as-a-Service' marketplace and sell their intelligence to other criminal groups.

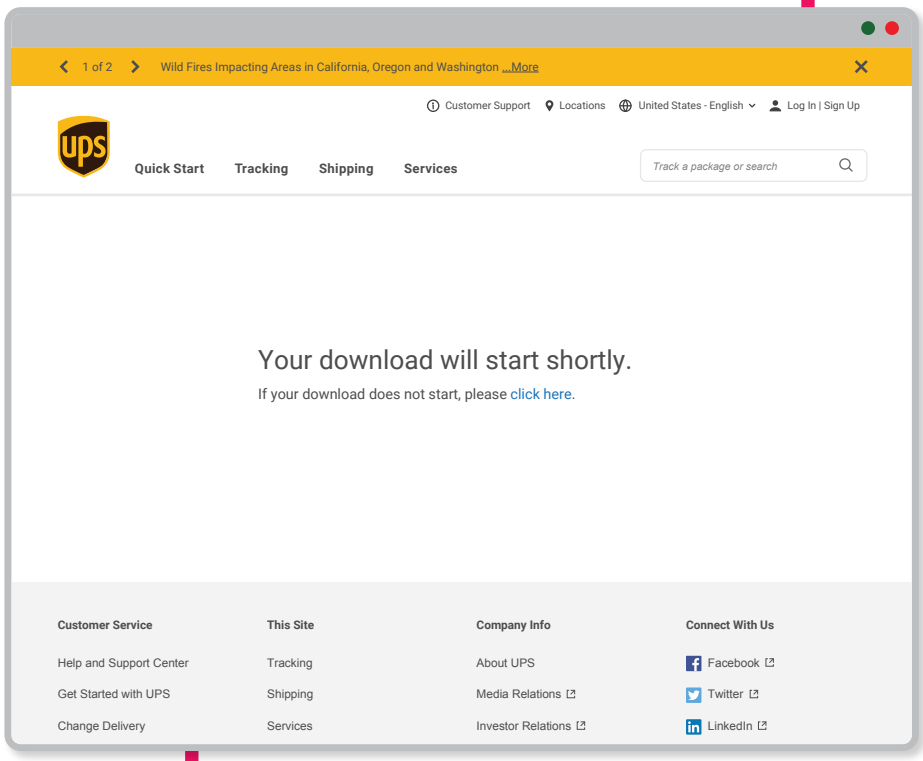


Image source: Bleeping Computer

All the links in the phishing emails were legitimate, except for the tracking number.

6 Un-happy birthday! e-Card scams

Surely scamming people on their birthdays is just mean… would cybercriminals sink that low? Of course they would! This new trend of exploiting flattery to trick people into clicking on malicious links has definitely caught our eye.

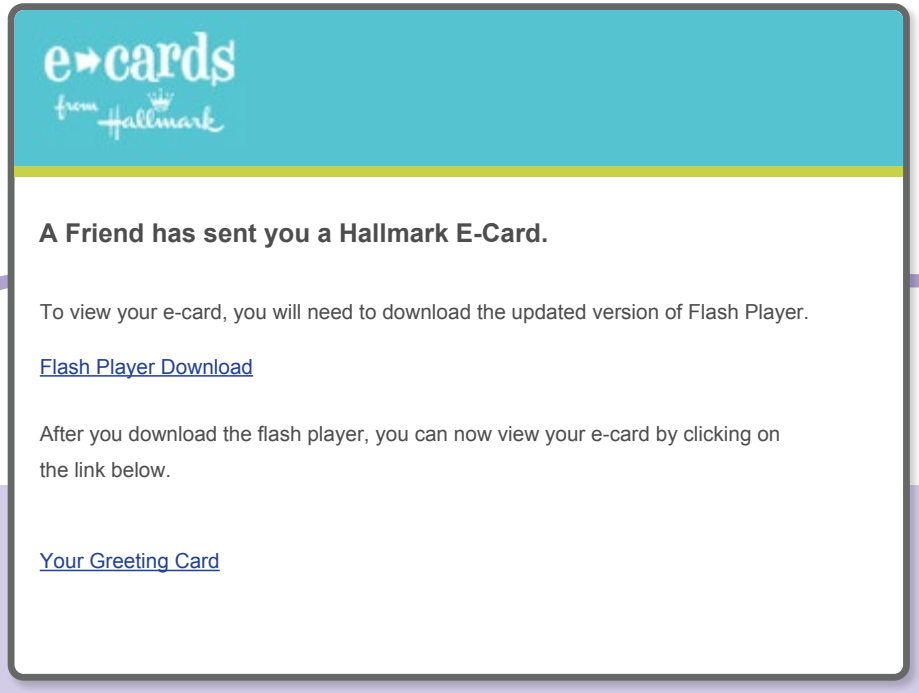


Image source: Beacon Bulletin

Attackers are using social media or other online sources to find out when people's birthdays are, and then sending them a link to "View your birthday e-card."

Unfortunately, the link doesn't bring up birthday wishes and Amazon vouchers – it's a weaponized phishing link that can contain malware or links to websites that will steal users' credentials.

It's a clever tactic. This scam catches people with their guard down, and entices them into clicking a (seemingly) low-risk link. If you're ever in doubt about an e-card – especially one from an unknown source – then we'd highly recommend you don't click to open it online.

Attackers are using social media or other online sources to find out when people's birthdays are

7 Safe with MFA? Don't be so sure...

There's a good reason so many businesses have adopted multi-factor authentication (MFA). Asking for two or more forms of authentication makes it much harder for hackers to compromise accounts. Even if they manage to steal a password, it's useless without a second piece of information like an SMS texted to a phone, an RSA token, or even a biometric identifier such as a fingerprint.

However, cybercriminals don't tend to sit on their hands and accept defeat.

We're seeing attackers find new ways to get around MFA. When a victim enters their credentials into a phisher's false web page, the attacker will log into their email account in real time. If they see MFA is enabled, they'll send the victim a request for their MFA credentials too, enabling them to bypass the protection it offers.

Some phishing emails contain a fake invite to view or edit a file. Once you've clicked the malicious link, a pop-up will offer a prompt along the lines of "Yes, give me access." What you've actually done is grant the hackers permanent access to your account – even if you change your password or have MFA enabled.

MFA is a valuable tool… but it's not foolproof.

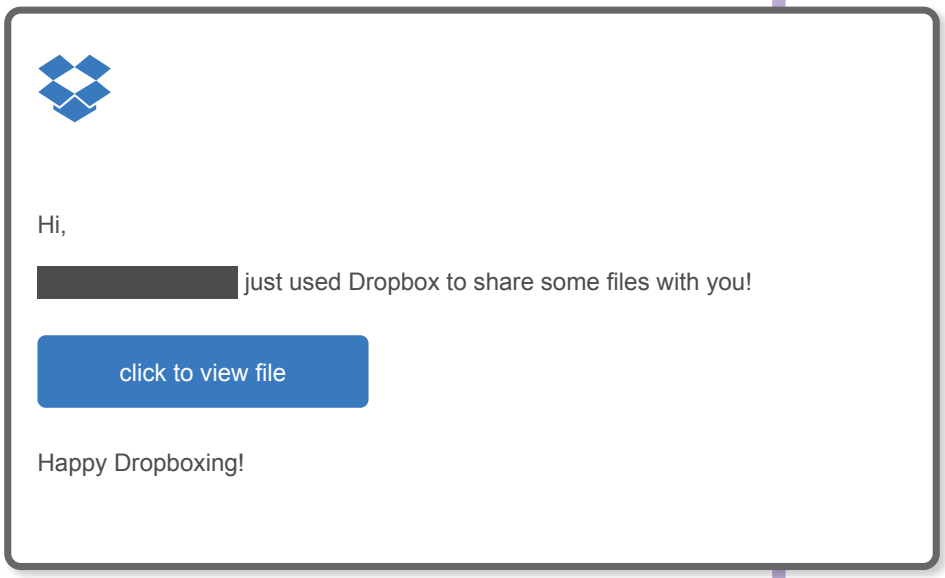


Image source: Spam Stops Here

Defending your people from phishing attacks

As you've seen throughout this whitepaper, there's no shortage of sophisticated and convincing phishing scams. We monitor the threat landscape closely and will keep you up-to-date on emerging scams – but please note these are just a few recent ones we've picked out as interesting. There are plenty more already out there.

These scams all have one thing in common: they're targeting the people in your organization. Your people are your last line of defense against phishing, but it's not fair to expect them to act as both detection and reporting mechanisms in the face of increasingly sophisticated and relentless targeted attacks.

It's time to implement intelligent security to defend employees where they need it most: directly in their inboxes.

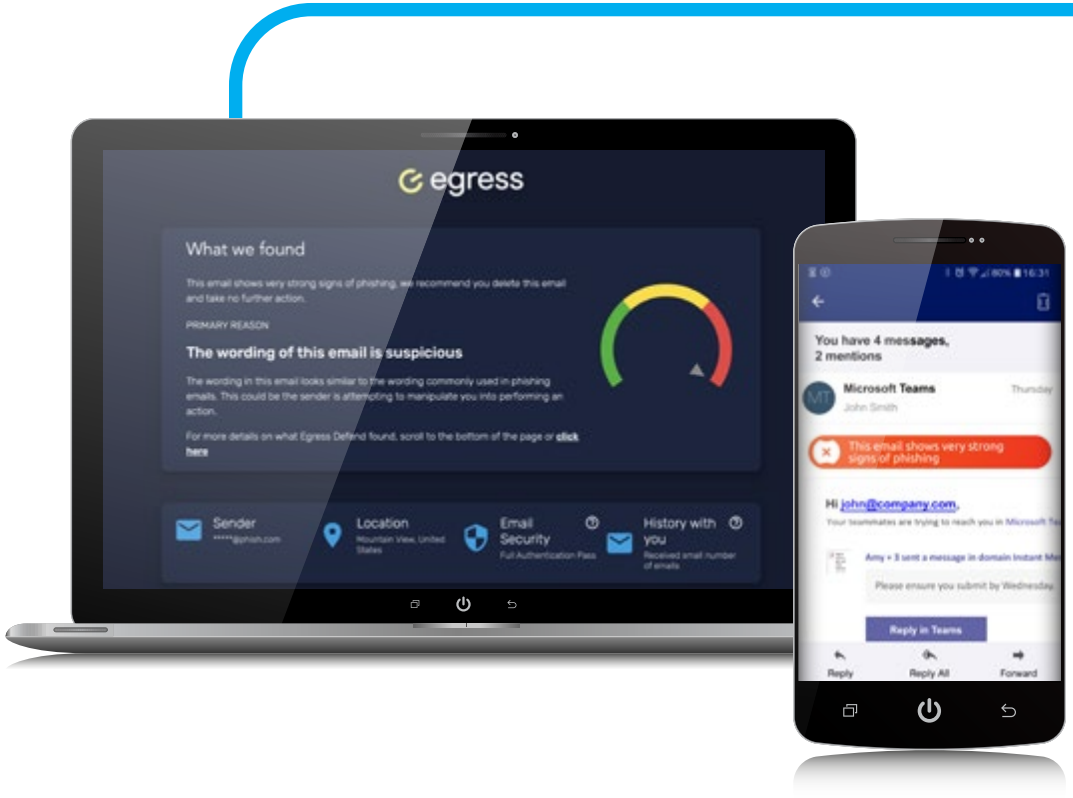
It's time to implement intelligent security to defend employees where they need it most: directly in their inboxes

Why Egress Defend?

Egress Defend is the only solution globally to operate on a zero-trust model for phishing detection, analyzing the context and content of every inbound email before it is delivered to employees' inboxes.

Deployed directly into Microsoft Outlook, Defend uses the latest in machine learning and natural language processing (NLP) technology to detect all types of phishing attacks, including the most convincing and therefore damaging ones, such as:

- Impersonation attempts and CEO fraud via spoofed domains
- Attacks that originate from compromised accounts on authenticated domains
- Attacks that utilize open-source intelligence (OSINT)
- "Payload-less" attacks that don't contain a malicious attachment or link but request an action be carried out, such a payment transfer
- Hyperlinks that are weaponized by cybercriminals post-delivery



Defend is also designed to partner with end-users for real-time active education. Using a traffic-light warning system and insight summaries, the solution alerts users to risk and provides "tooltip" explanations about phishing detection and why actions (such as clicking on a malicious link) are blocked.

The solution also offers administrators with comprehensive analytics and a real-time threat feed that spans the entire organization, so you can effectively monitor your phishing risk profile in real time.

Learn more about Defend

Book your Defend demo now

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats. Using patented contextual machine learning we detect and prevent abnormal human behavior such as misdirected emails, data exfiltration and targeted spear-phishing attacks.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York and Boston.

www.egress.com | info@egress.com | @EgressSoftware

egress