VIPRE Email Link Isolation Neutralises URL Threats and Educates Users

VIPRE®

36% of breaches involved phishing, **11%** more than last year.[1]

Email is the lifeblood of business communication. Companies recognise the strategic value of email, but there are risks: Cybercriminals are constantly developing more sophisticated attacks to scam busy, distracted, or trusting users. Email remains the primary attack vector for cyber threats from individual hackers, criminal organisations, and even nation-states. Email phishing attacks, the most common type of cyber-attack, grew an astonishing 1,100% from 2016 to 2020 because phishing has been so effective for attackers.

Ransomware, another rapidly growing threat category, doesn't just impact endpoint devices like laptops and workstations. Successful ransomware attacks can infect the entire network, restricting file, computer, and server access and even taking networks entirely offline. Overcoming the attack may result in significant productivity, financial, and reputational losses.

Email phishing attacks, the most common type of cyberattack, grew an astonishing 1,100% from 2016 to 2020.[2]

YOUR BUSINESS' PRIMARY COMMUNICATION METHOD DEMANDS PROTECTION

Once the domain of lone hackers, cybercrime is now big business as larger players approach and attack companies via email. The tried-and-true method of blocking known bad URLs and sandboxing attached files is no longer the only defence against attackers' evolving techniques. Each day there are new threats as hackers seek to access your confidential data, extract your financial assets, or even hold your systems hostage. Most organisations lack the time and resources to address these evolving threats, exposing them both legally and financially. Criminals are now increasingly looking for enticing opportunities within small- and medium-sized companies, school systems, and municipalities. They note that resource challenges in these organisations create security holes that are ripe for exploitation.

Email attacks threaten both IT staff and end-users. Businesses need a tool that can deliver industrial-strength protection on the front end, even against zero-day threats, and assist in the ongoing education of users as a follow-up to improve overall security. VIPRE Email Link Isolation is the only product to neutralise email threats and educate end-users, resulting in safer, more productive email usage. Email Link Isolation is part of VIPRE Advanced Threat Protection for Email and is also available as an add-on service for VIPRE Email Security Cloud.
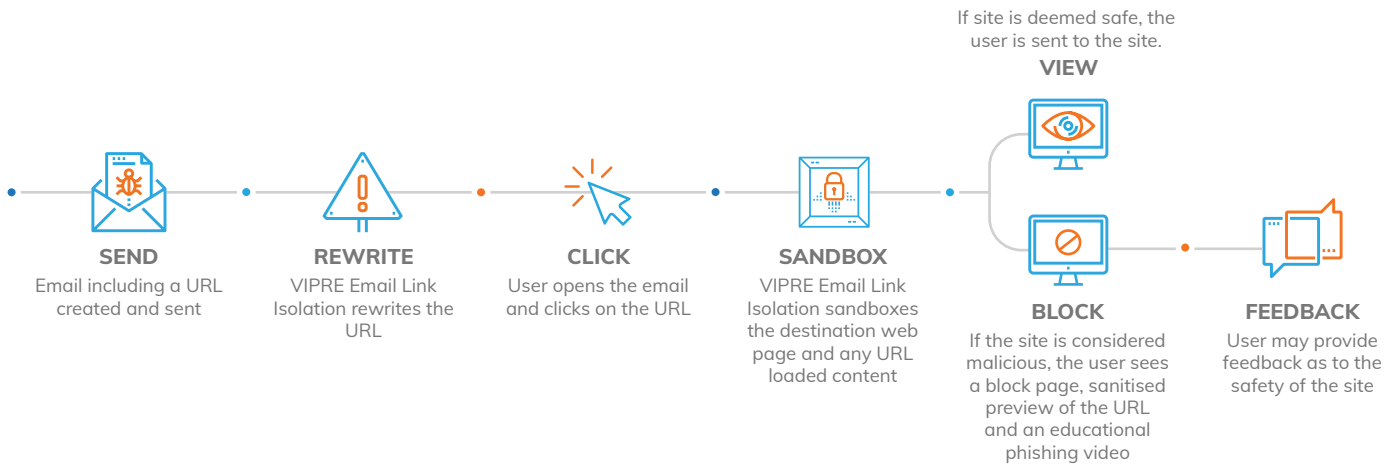
NEUTRALISING THE THREATS LIKE NO OTHER

VIPRE Email Link Isolation defends your email, your users, and your business through a potent set of capabilities designed to neutralise threats from cybercriminals' favourite attack vector – email. While criminals often attempt to camouflage phishing attacks by utilising authentic logos and branding, VIPRE sees through those tricks. It focuses on neutralising the threats, rendering even the most sophisticated attacks useless by the time they reach an end user's inbox.

By utilising URL rewriting, VIPRE Link Isolation immediately neutralises hidden threats from malicious URLs. When the email hits the inbox, it can no longer automatically launch a threat to compromise a device, network, or user. This capability protects against both known threats and suspicious URLs, staying far ahead of the simple allow/ deny lists that many other products in the market leverage. Because all links are rewritten, VIPRE also protects against cases where a legitimate website is compromised, a situation rarely detected by other products.

Criminals are now increasingly looking for enticing opportunities within small- and medium-sized companies, school systems, and municipalities. They note that resource challenges in these organisations create security holes that are ripe for exploitation.

LINK ISOLATION PROCESS

If site is deemed safe, the user is sent to the site.

VIEW

SEND
Email including a URL created and sent

REWRITE
VIPRE Email Link Isolation rewrites the URL

CLICK
User opens the email and clicks on the URL

SANDBOX
VIPRE Email Link Isolation sandboxes the destination web page and any URL loaded content

BLOCK
If the site is considered malicious, the user sees a block page, sanitised preview of the URL and an educational phishing video

FEEDBACK
User may provide feedback as to the safety of the site

A deep scan of the message content, including all the hidden and embedded components, is performed through a click-time interception to ensure the message's validity. This scan comprehends the entire chain, from the inbox back to any linked web servers or services.

VIPRE Link Isolation includes cloud sandboxing of URLs and webpages for additional protection. Cloud sandboxes are not a new concept, but many security products use sandboxes in a limited way to only handle email file attachments. VIPRE excels by extending the reach and impact of the cloud sandbox to isolate the entire message and all included URLs. By securely sandboxing the embedded URLs in an email message, the product delivers enhanced protection, even if a user accidentally clicks an embedded or hidden link.

While many email security products can protect against known threats, the ever-expanding world of cybercrime has become even more sophisticated, often launching new web services in conjunction with phishing-embedded emails. These zero-day threats provide an increased challenge for IT departments, which can rarely stay on top of every new vector or method. But Email Link Isolation stands out in addressing zero-day threats. This powerful security tool is rewriting all the links, sandboxing URLs, and their landing pages, intercepting clicks, and providing live feedback about threats. Even if a new, malicious, and unknown server comes online as the phishing emails are released, the product can catch these threats, preventing zero-day attacks from infiltrating your systems.
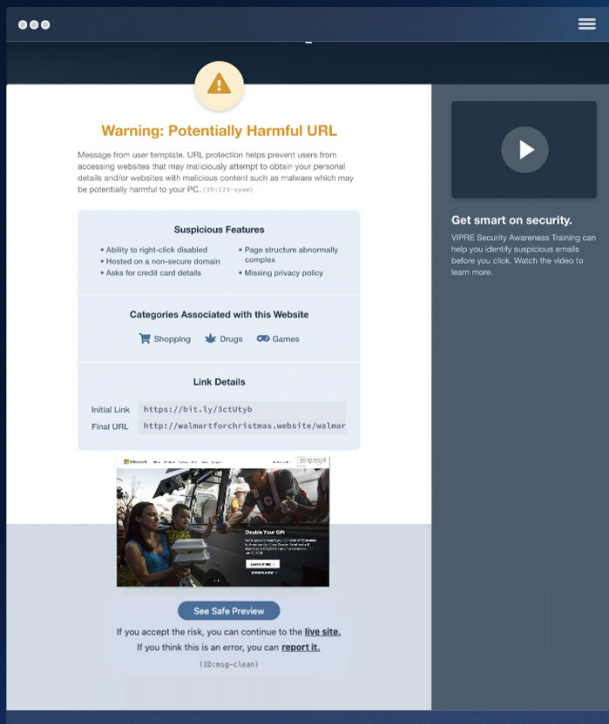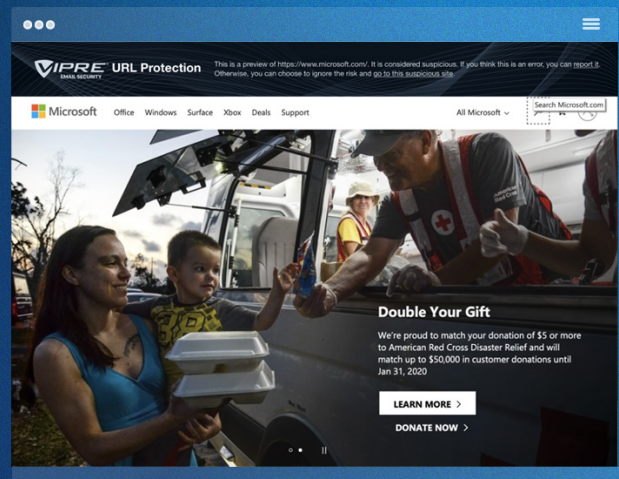
SANITISED PAGE ·······················

BLOCK PAGE ·······················

EDUCATION – THE OTHER HALF OF THE BATTLE

Despite all the additional layers of security Link Isolation brings to the IT toolbox, intelligent tools alone cannot solve the problem of email safety because human behaviour and user error detrimentally affect overall security. Link Isolation is uniquely designed to address both the technical side of email security and the human side at the point of failure.

When an email message with a questionable link or content is opened by an end-user, that user will immediately receive a block page explaining the suspicious link. They will also receive education regarding the threat. This detailed information, delivered as the threat is neutralised, helps inform the user and diminishes the probability they will be susceptible to similar attacks in the future.

Additionally, the user will watch an educational phishing video to drive the lesson home. Interactive engagement via our award-winning training videos increases the efficacy of the training and improves your organisation's security posture.

Users may sometimes encounter false positives. Suppose the end-user believes that the URL is safe despite the warnings provided. In that case, VIPRE Link Isolation will generate a sanitised live preview of the page to show the content of the destination URL, highlight potential issues with the page, and allow the user to provide feedback to the IT staff if they believe that the page is legitimate. The IT administrator will then have an opportunity to view the input and determine how to act. If they agree that the resulting page is safe, a revised email is sent back to the end user's inbox without the rewritten URLs. All response templates to address user reports can be customised to match the specific needs of your business.

VIPRE Link Isolation is a powerful tool that supports IT departments with the best technology advancements like click-time interception and cloud sandboxing. Its straightforward and streamlined configuration process requires only a few clicks. Once activated, VIPRE Email Link Isolation works to protect against all the attacks that cybercriminals might throw at you, including zero-day attacks. But then this tool takes the next step: It educates users at the point of attack, empowering users to spot the traps for themselves.

PROTECT YOUR BUSINESS; PROTECT AND EDUCATE YOUR USERS

Email is the most important communication channel for most businesses, but it's also your area of greatest risk. Protect your email, your users, and your business. You need a powerful tool to counter the complexity and sophistication of cyberattacks. VIPRE Link Isolation takes email protection to the next level by both neutralising threats and educating end users.

VIPRE Link Isolation is an integral part of VIPRE's Email Advanced Threat Protection service, a comprehensive security package that helps protect your business from phishing, viruses, malware, ransomware, and other outside attacks. Organisations already utilising VIPRE Email Security Cloud can easily add VIPRE Link Isolation to their existing service subscription and take advantage of its power and thoughtful education to better secure their business.

---

1   https://www.verizon.com/business/en-gb/resources/reports/dbir/
2   FBI IC3 Annual report, 2020 https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

ELEVATE YOUR EMAIL PROTECTION with VIPRE Link Isolation and take a truly holistic approach to email security.

FOR MORE INFORMATION visit global.VIPRE.com or call +44 (0) 800 093 2580 or send email to uksales@VIPRE.com.

VIPRE®