US SIGNAL®

AVOID BEING ANOTHER STATISTIC WITH US SIGNAL'S ADVANCED EMAIL SECURITY

POWERED BY PERCEPTION POINT + ACRONIS

TABLE OF CONTENTS

THE NUMBERS TELL THE STORY

The statistics don't lie. Approximately 94% of cyber-attacks are carried out via email. It's estimated that 3.4 billion phishing emails are sent out each day around the world. Almost half of all the emails sent in 2021 were phishing emails. As if that weren't enough, phishing causes approximately 90% of data breaches.

With all the email security solutions on the market, why are email threats still such a serious problem? For one thing, many companies don't take the time to reevaluate the capabilities and effectiveness of their current solutions. Nor do they investigate new technologies.

There are also those organizations that simply choose to rely on the basic email hygiene capabilities of Google and Microsoft. Despite these companies investing and updating their security capabilities, they're often limited in what they offer.

Cybercriminals also continue to become more sophisticated and innovative. Their methods are always evolving.

One solution to the dilemma: US Signal's Advanced Email Security. Keep reading to learn what it can do – and how.

PROTECT CLOUD MAILBOXES AND MAIL SERVERS

Advanced Email Security protects cloud mailboxes such as Microsoft 365, Google Workspace, and Open-Xchange without any need for additional configurations during initial deployment. It can also be used for protecting on-premises mail servers, but this requires MX record configurations.

COMMON TYPES OF EMAIL SECURITY

Content disarm and reconstruction (CDR):
This process breaks down suspicious attachments into their constituent parts, stripping out elements that may pose a threat, and rebuilding them into a safe version. It removes any element of a file that doesn't align with your company's security parameters, which means it protects against new threats that other mechanisms may not recognize.

Domain-based message authentication, reporting and conformance (DMARC):
This is a protocol to authenticate that inbound emails from a specific domain are using that domain legitimately. DMARC can be highly effective in defending your business against fraudulent messages.

Network sandbox:
Using a network sandbox, security professionals can analyze attachments in an isolated coding environment where they pose no threat to your core business network. The idea is to test attachments that aren't explicitly dangerous but might still pose a threat.

Remote browser isolation (RBI):
RBI sends users to an external browser when they click on a suspicious link, ensuring that security risks are isolated from the business network. Users can only interact with clean website content because dangerous content is not rendered for them to see.

Anomaly detection:
Anomaly detection uses telemetry and data intelligence to detect deviations from normal email behavior that point to advanced forms of spam and phishing.

URL rewriting and time-of-click analysis:
By rewriting suspicious URLs before they're delivered, the link is either converted into a non-clickable version, thus disarming it; removed from the message entirely; or redirected to an inspection service for time-of-click analysis.

COMBAT PHISHING

It's been reported that phishing attacks are the root of 91% of all cyberattacks. Leveraging social engineering, the cybercriminals behind these attacks deceive their targets and gain access to sensitive information by employing files, URLs, and text-based techniques posing as legitimate sources.

Advanced Email Security helps prevent phishing before it reaches end-users using:

+ Anti-evasion technology that detects malicious hidden content by recursively unpacking the content into smaller units (files and URLs)
+ An image recognition engine that blocks unknown malicious URLs based on the images and logos used on webpages
+ Threat intelligence delivered via six market-leading sources and a unique engine that scans URLs and files
+ URL reputation – To block known malicious URLs based on four leading URL reputation engines

TYPES OF PHISHING ATTACKS

Spear Phishing.
The attacker uses information about a single target to make a request for information seem as natural and believable as possible. For example, it might target a company manager by emailing about a conference attended recently and attaching a document purporting to be about the event but that contains malicious code.

Whaling.
It's similar to spear phishing, but has a bigger target: company executives. Attackers specifically target them because they have access to more data and financial accounts than lower-level employees. This kind of attack is all about getting as much money and data as possible from a single hit.

Clone / Deceptive Phishing.
An email is received from a well-known online brand. It includes the company logo and an email address that passes for the real thing. The target is asked to click a link and then is taken to the brand's site where the target is directed to log in. The problem is, it wasn't the real site – and any password entered goes to the phisher.

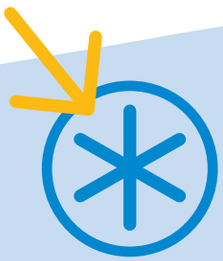
TAKE ON BUSINESS EMAIL COMPROMISES (BEC)

Impersonation-based attacks trick employees into thinking they're communicating with someone they know so they'll make a mistake — a mistake that results in initiating a wire transfer or giving away sensitive information. A significant part of BEC attempts don't have a malicious payload and leverage only text-based techniques, making them especially tricky to detect and prevent.

Advanced Email Security helps prevent impersonation attempts with:

+ **Anti-evasion** – Deep scan to detect malicious hidden content
+ **Anti-spoofing** - Prevent payload-less attacks through machine-learning algorithms with IP reputation, SPF, DKIM, and DMARC record checks
+ **Payload-based Protection** – Reduce "further along the line" BEC attacks with threat intelligence, phishing, and antivirus engines

STEP 1:
IDENTIFY A TARGET



Organized crime groups target businesses in the US and abroad by exporting information available online to develop a profile on the company and its executive.

STEP 2:
GROOM THE VICTIM

Phising emails or phone calls target a victim company's officials. Perpetrators use persuasion and pressure to exploit employees.

STEP 3:
EXCHANGE INFO

The victim is convinced they are conducting a legitimate business transaction. The unwilling victim is then provided wiring instructions.

STEP 4:
WIRE TRANSFER

Upon transfers, the funds are steered to a bank account controlled by the organized crime group.

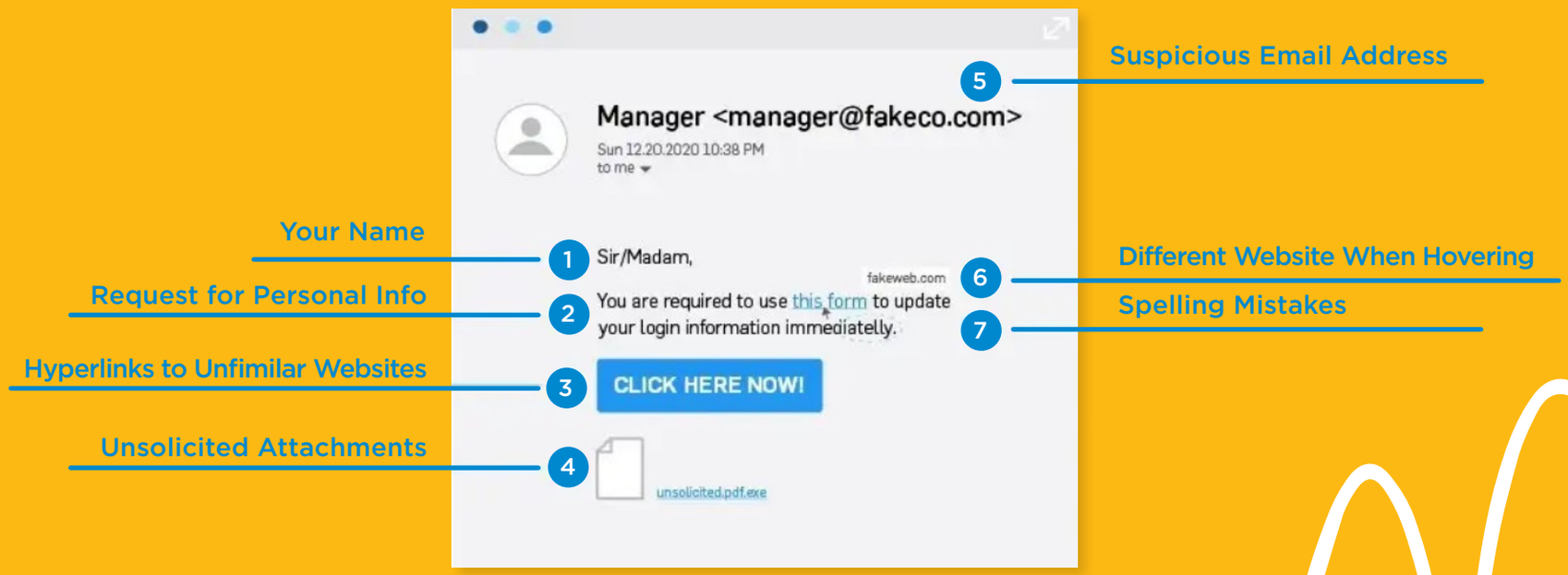
HALT INTERNAL PHISING

Internal phishing can result from account takeovers, malicious employees, or even human error. Legacy technologies commonly neglect internal emails, as scanning 100% of traffic results in delays in email delivery or damages files and URLs.

Advanced Email Security prevents account takeover attempts and internal phishing with:

+ Anti-evasion – Detect malicious hidden content
+ Image recognition engine – Block unknown malicious URLs based on the images
+ Next-generation dynamic engine – Catch zero-days and APTs that evade conventional defenses
+ Scanning of 100% of traffic – Unique speed allows scanning all internal and inbound emails
+ URL reputation engines - Block known, malicious URLs and logos used on web pages

7 SIGNS OF A PHISING EMAIL



PREVENT ZERO-DAYS AND APTS

Zero-days and APTs are particularly stealthy. They can lie in wait and then strike by leveraging unknown software vulnerabilities. It can take months before they're discovered. Standard APT modules, such as sandboxes or content disarm and reconstruction solutions (CDRs), rely on known data and behaviors that evasion techniques can mask when in a sandbox.
Advanced Email Security helps prevent zero-days and APTs with:

+ Unique CPU-level technology that detects and blocks advanced attacks at the exploit stage, before malware release, based on the assembly code. Exploits are blocked before the malware is released and a clear verdict is delivered in seconds.

HOW AN APT WORKS

An Advanced Persistent Threat (APT) gains ongoing access to the system in five steps: Hackers achieve this in a series of five stages:

GAIN ACCESS → ESTABLISH A FOOTHOLD → DEEPEN ACCESS → MOVE LATERALLY → LOOK, LEARN, + REMAIN

DETECT EVASION TECHNIQUES

Email-borne attacks are increasingly difficult to detect. Attackers use evasion techniques, such as new file types, link chains, malicious content hidden within clean files, and stalling mechanisms that sandboxes can't observe, ensuring the malicious payload takes action only when facing actual end-users. For conventional defenses, preventing such techniques is almost impossible as it takes too much time, money, and technological resources.

Advanced Email Security employs a unique technology to prevent evasion techniques that conventional defenses miss:

+ Anti-evasion - Recursively unpack the content into smaller units, which are then dynamically checked by multiple engines in under 30 seconds, compared to 20+ minutes for legacy sandboxing solutions.

Common Email Evasion Techniques

+ Brand impersonation with procedurally generated graphics
+ Link chains
+ Malicious content hidden within clean files
+ New file types
+ Stalling code
+ Text padding with invisible characters
+ Victim-specific URI
+ Zero-point font obfuscation

ENHANCE MICROSOFT 365 DEFENSES

Organizations are increasingly dissatisfied with the native defense capabilities of Microsoft 365, as they are slow to detect issues and unable to prevent more advanced attack techniques. **Advanced Email Security** ensures all email-borne threats are blocked in seconds.

ADVANCED EMAIL SECURITY VS MICROSOFT 365 SECURITY

	ADVANCED EMAIL SECURITY	MICROSOFT 365
Detection Speed	< 30 seconds	5 - 20 Minutes
Detection Accuracy	Best-in-Class	Below Average
Threat Coverage	Best-in-Class	Limited
Detection of Malicious URLs	Best-in-Class	Average
Detection of Zero-Days	Best-in-Class	Limited
Prevention of APTs	Included	N/A
Anti-Evasion	Included	N/A
Incident Response Services	Included	N/A

LEADING-EDGE TECHNOLOGIES MAKE THE DIFFERENCE

US Signal's **Advanced Email Security** combines a full array of defense and risk mitigation technologies and strategies to offer the most comprehensive email security, including:

Anti-phishing Engines
Detects malicious URLs based on leading reputation engines, along with advanced image recognition technology to validate URL legitimacy.

Anti-spoofing
Prevents payload-less attacks — including look-alike domains, spoofing, and display name deception — through the use of machine-learning algorithms with IP reputation, SPF, DKIM, and DMARC record checks.

Fast Scanning
Detects malicious hidden content by recursively unpacking the content into smaller units (files and URLs). They're dynamically examined by multiple engines in under 30 seconds – faster than legacy sandboxing solutions that can take more than 20 minutes.

Next-generation Dynamic Detection
Stops advanced attacks such as APTs with CPU-level analysis that detects and blocks them at the exploit stage by identifying deviations from normal execution flow during runtime.

Spam Filter
Blocks malicious communications with anti-spam and reputation-based filters that draw on data from several advanced technologies.

Static Signature-based Analysis
Identifies known threats with best-in-class, signature-based AV engines enhanced with a unique tool to identify highly complex signatures.

Threat Intelligence
Stays on top of emerging threats with the combined threat intelligence of market-leading sources and a unique engine that scans URLs and files.

Incident Response Service
Provides direct access to cyber analysts who act as an extension of your service delivery team. In addition to monitoring all customer traffic and analyzing malicious intent, they provide ongoing reporting and support, including handling false positives, remediating, and releasing when required.

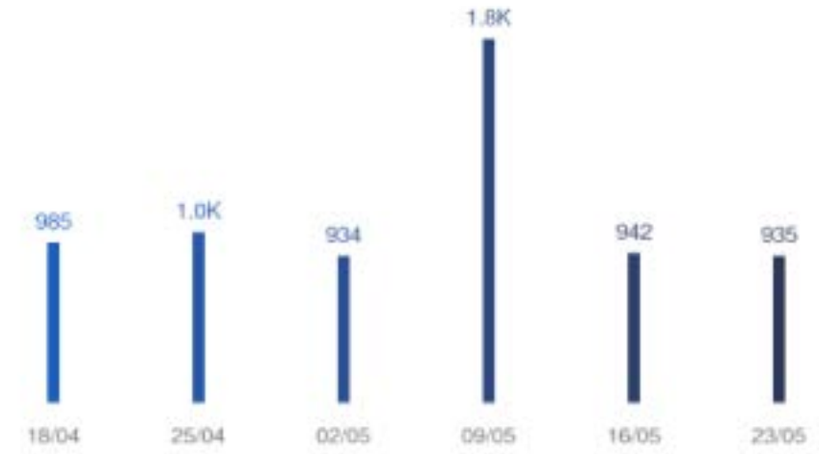
SAMPLE INCIDENT REPORT

947 INCIDENTS

1.8K ITEMS SCANNED

SPAM	MALICIOUS
941	6

TOTAL INCIDENTS PER WEEK



TOP ATTACKING DOMAINS/SENDER

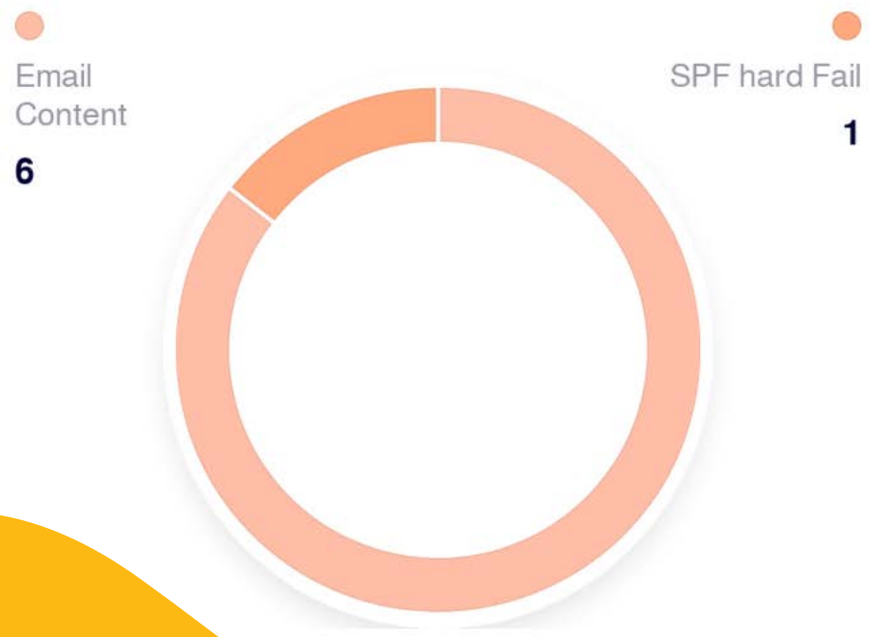
Your Name voicemail@youmail.com	2
"software work (youmail)" voicemail@youmail.com	1
"tina klap (youmail)" voicemail@youmail.com	1

MOST ATTACKED PEOPLE

yourname@yourcompany.com	6 →

LAYERS

TOP ENGINES



THE EXTRAS

The features and capabilities of US Signal's Advanced Email Security are further bolstered by:

24/7/365 US Signal Support

+ The US Signal Technical Operations Center (TOC) provides all support for US Signal customers.

Licensing

+ Licensed per unique user; shared and group mailboxes are not charged separately

Continuous Monitoring

+ An expert intelligence team continuously monitors incidents.

Best-in-Breed Technologies

+ Technologies include machine-intelligence-enhanced Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) record checks. Few, if any, solutions integrate so many different best-in-class technologies.

TAKE ACTION NOW!

There’s no sign of cybercriminals slowing down their email attacks. That doesn’t mean your organization has to fall victim to them. Enhance your cyber protection services with one of the most comprehensive, proactive solutions available: US Signal’s Advanced Email Security. It’s powered by US Signal’s technology partners Perception Point and Acronis.

Learn more about US Signal’s full range of IT security solutions at: **ussignal.com/services/security-services**

US SIGNAL®