N-ABLE™

Technologies of Trust:

Protecting Against Email Fraud and Scams

Email has long been one of the primary methods used by cybercriminals—in fact, it's the #1 attack vector[1]

96% of social attacks (phishing and pretexting) infiltrate through email [2]

73% of the time **cloud breaches** involved email or web application servers [3]

$26 billion was reported in **losses** due to **business email compromise** (BEC) [4]

BEC and spoofing are **two of the top three** cybercrime types in terms of fiscal losses [5]

Most scammers try to trick people via impersonation. They use sophisticated techniques to craft email attacks, like:

- Forging a sender display name or the "from" email field to make it appear that an email comes from a trusted recipient (i.e., display name spoofing)
- Forging a sender email domain to make the recipient believe the email is coming from a legitimate or trusted company (i.e., domain name spoofing)
- Changing the "From," "Envelope-From," and "Reply-To" addresses—e.g., From: <john@example.com>, Reply-To: john <examplegmail@gmail.com> (i.e., attribute spoofing)

Email security protocols can help combat vulnerabilities inherent in email. A few examples:

Domain Keys Identified Mail (DKIM):

Helps verify an email was sent from the domain it claims to be from.

- Reduces the chances of emails being identified as spam
- Helps discourage others from spoofing your email

Sender Policy Framework (SPF):

Helps make sure an email comes from a legitimate source.

- Helps receiving email servers verify an incoming email comes from an IP address approved by the sender
- Best used in combination with the DMARC and DKIM

Domain-Based Message Authentication, Reporting, and Conformance (DMARC):

Works in concert with both DKIM and SPF and helps the sender specify which framework they're using when sending email—SPF, DKIM, or both.

- Helps the sender specify how to treat emails that don't authenticate, including quarantining, rejecting, or deleting them
- Helps senders actively warn users that someone is attempting to phish them using your domain name

Email authentication alone is not enough.

Cybercriminals can still get past these checks using several methods (e.g., registering lookalike domains and configuring SPF, DKIM, and DMARC).

Using advanced email analysis techniques—that evaluate both the origin and context of email—is key to strong email protection.

Prevention checklist:

- ✓ Sender authentication (SPF I DMARC I DKIM)
- ✓ IP reputation
- ✓ Header inspection
- ✓ Domain reputation
- ✓ Domain and link analysis
- ✓ RFC alignment
- ✓ Content checks

The N-able™ Mail Assure solution offers proprietary email filtering technology that can help strengthen your email security posture.

learn more

About N-able

N-able (formerly SolarWinds MSP) empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale. n-able.com

1 "2019 Data Breach Investigations Report," Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf (Accessed June 2020).
2 "2020 Data Breach Investigations Report," Verizon. https://enterprise.verizon.com/en-nl/resources/reports/dbir/ (Accessed June 2020).
3 "2020 Data Breach Investigations Report," Verizon. https://enterprise.verizon.com/en-nl/resources/reports/dbir/ (Accessed June 2020).
4 "2019 Internet Crime Report," Federal Bureau of Investigation. https://pdf.ic3.gov/2019_IC3Report.pdf (Accessed June 2020).
5 "2019 Internet Crime Report," Federal Bureau of Investigation. https://pdf.ic3.gov/2019_IC3Report.pdf (Accessed June 2020).