VIEWPOINT 2021 MAR 12

EMAIL SECURITY SETTINGS: ARE YOURS ACTIVATED?

WESTWARD'S VIEW

Cyber attacks are on the rise. As technology becomes more advanced, so do the tricks scammers use to deceive and defraud their victims. The average cost of a data breach in Canada for 2020 was $4.5 million, and the average time to identify and contain a breach was 226 days[1].

In this Viewpoint, we share Westward's "Top 6" email security settings and encourage all our clients and colleagues to activate these settings to help protect email communications from attack.

The opinions expressed in this memorandum are strictly those of Westward Advisors Ltd. This memorandum is for information purposes only and is not legal or tax advice.

THE ISSUE

Scammers are able to *"spoof"* legitimate email addresses, making it look like their email is from a reputable source. For example, a scammer could send an email to a Westward client that appears to the recipient as coming from a legitimate *trustedname@westwardadvisors.com* email address.

If the recipient's email security settings are not activated then the email will likely pass through to the recipient. The email contains fraudulent instructions from a supposedly trusted source to, for example, **redirect an upcoming life insurance premium wire transfer to the attacker's bank account.**

Hopefully, the recipient questions the authenticity of the email and independently contacts the alleged Westward source to verify these unusual instructions, however **properly activated email security settings will help prevent such a fraudulent email** from passing through to the recipient in the first place.

OUR TOP 6 EMAIL SECURITY SETTINGS

- Disable "Safe Senders"
- Disable external email forwarding
- Enable SPF
- Enable DKIM
- Enable DMARC
- Enable DNSSEC

These are activated on Westward's email ecosystem to protect ourselves and our clients and colleagues. When **both** the email sender and the email receiver have activated these email security settings, protection against potentially costly cyber attacks is greatly enhanced.

Since there is no foolproof security setting, employee education can go a long way to identifying and preventing fraud when the attackers get through the technology defenses. Web based third party employee training programs are becoming a cost-efficient solution. Westward uses KnowBe4.com to deliver security awareness and training on a continuous basis to the entire employee group, including random anonymous "tests" to evaluate employee awareness levels.[3]

© Copyright 2020-21 Westward Advisors Ltd. All rights reserved.
The LifeStep Process is a registered trademark of Westward Advisors Ltd.

WESTWARD'S TOP 6 EMAIL SECURITY SETTINGS

SETTING[2]	WHY?
Avoid "Safe Senders" and "Allowed Domains"	**Prevent attackers from bypassing Westward email security settings.** When system Users save email addresses in "Safe Sender" lists and domains in "Allowed Domain" lists, incoming fraudulent email spoofing a safe sender or domain is likely to bypass all email security settings. For more information, see *this Microsoft article*. Westward has a policy prohibiting employees from using Safe Sender lists or Allowed Domain lists in their Outlook email settings. Our IT administrator monitors User Safe Sender lists and Allowed Domain lists and removes all entries from User profiles.
Disable external email forwarding	**Prevent attackers from capturing copies of inbound email to Westward.** When system Users are tricked into clicking a fraudulent link, it may secretly install an email forwarding rule in the User's email profile. The rule is continuously searching for and forwarding emails to the attacker that contain targeted terms like ***"wire," "transfer," "payment,"*** etc. Westward has disabled external email forwarding on our email server to override any User rules attempting to automatically forward incoming email to someone outside the organization.
Enable SPF *(Sender Policy Framework)*	**Prevent attackers from spoofing Westward source email from an unauthorized email server.** SPF is an open standard which allows the domain owner to publish a list of email servers allowed to send email from that domain. Westward has activated SPF and published the servers authorized to send our email. Recipient spam filters detecting an unauthorized source of an alleged Westward email are likely to block the spoofed email.
Enable DKIM *(DomainKeys Identified Mail)*	**Prevent attackers from altering outbound emails in transit from Westward.** DKIM is an open standard designed to make sure messages are not altered in transit between the sending and recipient servers using an encrypted digital key created by the sending email server and decoded by the recipient email server. Westward has activated DKIM to improve the security and trustworthiness of outbound email.
Enable DMARC *(Domain-based Message Authentication Reporting and Conformance)*	**Instruct recipients to reject inbound emails from Westward that fail SPF and DKIM.** DMARC tells an email recipient whether the alleged originating domain of the incoming email message is protected by SPF and DKIM, and what to do if SPF and DKIM verification fails. Westward has enabled DMARC and set instructions to recipients of email from Westward to reject the email if the recipient's email server detects a SPF or DKIM failure.
Enable DNSSEC	**Prevent attackers from intercepting inbound email to Westward.** The Domain Name System (DNS) translates a human friendly internet address to the matching machine friendly internet IP address. Internet traffic is routed through many servers to reach the target destination, and those servers are using DNS to deliver the traffic to the correct internet destination such as an email server or a website. Enabling DNSSEC secures an organization's domain name and IP match in the public Domain Name System. Westward has activated DNSSEC to help prevent unauthorized interception of emails inbound to Westward.

[1] IBM Security, July 2020, "Costs of a Data Breach Report 2020", IBM [online] available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf
[2] This is a partial list. See the complete list at: https://www.upguard.com/blog/the-email-security-checklist
[3] Westward does not derive any benefit from referencing KnowBe4.

The opinions expressed in this memorandum are strictly those of Westward Advisors Ltd. This memorandum is for information purposes only and is not legal or tax advice.

© Copyright 2020-21 Westward Advisors Ltd. All rights reserved.
The LifeStep Process is a registered trademark of Westward Advisors Ltd.