CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

EMAIL CYBERSECURITY CHEAT SHEET

① Email Security

Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise.

- Email is a popular medium for the spread of malware, spam, and phishing attacks, using deceptive messages to entice recipients to divulge sensitive information, open attachments or click on hyperlinks that install malware on the victim's device.
- Email is also a common entry vector for attackers looking to gain a foothold in an enterprise network and breach valuable company data.
- Email security is necessary for both individual and business email accounts, and there are multiple measures organizations should take to enhance email security.

② Necessity of Email Security

Due the popularity of email as an attack vector, it is critical that enterprises and individuals take measures to secure their email accounts against common attacks as well as attempts at unauthorized access to accounts or communications.Malware sent via email messages can be quite destructive. Phishing emails sent to employees often contain malware in attachments designed to look like legitimate documents or include hyperlinks that lead to websites that serve malware. Opening an email attachment or clicking on a link in an email can be all that it takes for accounts or devices to become compromised.

Necessity of Email Security (con't) ②

Phishing emails can also be used to trick recipients into sharing sensitive information, often by posing as a legitimate business or trusted contacts. Phishing attacks against businesses often target departments that handle sensitive personal or financial information, such as accounts payable or human resources. In addition to impersonating known vendors or company executives, attackers will try to instill a sense of urgency in phishing emails to increase their chances of success. Phishing emails aimed at stealing information typically will ask recipients to confirm their login information, passwords, social security number, bank account numbers, and even credit card information. Some even link to counterfeit websites that look exactly like that of a reputable vendor or business partner to trick victims into entering account or financial information.

Continue reading on next page >

EMAIL CYBERSECURITY CHEAT SHEET

(CONTINUED)

③ Email Security Policies

Because email is so critical in today's business world, organizations have established policies around how to handle this information flow. One of the first policies most organizations establish is around viewing the contents of emails flowing through their email servers. It's important to understand what is in the entire email in order to act appropriately. After these baseline policies are put into effect, an organization can enact various security policies on those emails.These email security policies can be as simple as removing all executable content from emails to more in-depth actions, like sending suspicious content to a sandboxing tool for detailed analysis. If security incidents are detected by these policies, the organization needs to have actionable intelligence about the scope of the attack. This will help determine what damage the attack may have caused. Once an organization has visibility into all the emails being sent, they can enforce email encryption policies to prevent sensitive email information from falling into the wrong hands.

Email Security Tools ④

A secure email gateway, deployed either on-premises or in the cloud, should offer multi-layered protection from unwanted, malicious and BEC email; granular visibility; and business continuity for organizations of all sizes. These controls enable security teams to have confidence that they can secure users from email threats and maintain email communications in the event of an outage.

An email encryption solution reduces the risks associated with regulatory violations, data loss and corporate policy violations while enabling essential business communications. The solution should work for any organization that needs to protect sensitive data, while still making it readily available to affiliates, business partners and users—on both desktops and mobile devices. An email encryption solution is especially important for organizations required to follow compliance regulations,.

Continue reading on next page >

EMAIL CYBERSECURITY CHEAT SHEET

⑤ Business Best Practices

There are multiple ways to secure email accounts, and for enterprises, it's a two-pronged approach encompassing employee education and comprehensive security protocols.

Best practices for email security include:

- Engage employees in ongoing security education around email security risks and how to avoid falling victim to phishing attacks over email.
- Require employees to use strong passwords and mandate password changes periodically.
- Utilize email encryption to protect both email content and attachments. (Typically TLS.)
- Implement security best practices for BYOD if your company allows employees to access corporate email on personal devices.
- Ensure that webmail applications are able to secure logins and use encryption.
- Implement scanners and other tools to scan messages and block emails containing malware or other malicious files before they reach your end users.
- Implement a data protection solution to identify sensitive data and prevent it from being lost via email.

(CONTINUED)

Individual Best Practices ⑥

There are also some important best practices that end users should follow to ensure secure email usage. Arming your employees with the know-how to avoid risky behaviors can make a substantial impact on your company's ability to reduce risks associated with email.

- Email security best practices for end users/employees include:
- Never open attachments or click on links in email messages from unknown senders.
- Change passwords often and use best practices for creating strong passwords.
- Never share passwords with anyone, including co-workers.
- Try to send as little sensitive information as possible via email, and send sensitive information only to recipients who require it.
- Use spam filters and anti-virus software.
- When working remotely or on a personal device, use VPN software to access corporate email.
- Avoid accessing company email from public wi-fi connections.

By educating employees on email security and implementing the proper measures to protect email, enterprises can mitigate many of the risks that come with email usage and prevent sensitive data loss or malware infections via email..

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH