CSNP
CYBERSECURITY NON-PROFIT

Email Security Guide for Business

A comprehensive guide to protecting your organization from email threats

CSNP RESOURCE

FREE GUIDE

CHAPTER 1

Understanding the Email Threat Landscape

Email remains the primary attack vector for cybercriminals, with over 90% of successful cyberattacks starting with a malicious email. The threat landscape continues to evolve with increasingly sophisticated tactics.

Most Common Email Threats

- Phishing attacks targeting credentials and sensitive data
- Business Email Compromise (BEC) scams
- Malware and ransomware distribution
- Spoofing and impersonation attacks

Recognizing Phishing Attempts

Phishing emails disguise themselves as legitimate communications to steal information or install malware. Learn to spot the warning signs before it's too late.

Suspicious Sender Address

Check for slight misspellings in email domains like "micr0soft.com" or unusual sender addresses that don't match the company name.

Urgent Language & Pressure

Phrases like "Act now!" or "Account suspended" create artificial urgency to bypass your critical thinking.

Suspicious Links & Attachments

Hover over links to reveal the true destination URL. Be wary of unexpected attachments, especially .exe, .zip, or macro-enabled documents.

Poor Grammar & Formatting

Professional organizations rarely send emails with spelling errors, awkward phrasing, or inconsistent branding.

Business Email Compromise (BEC)

BEC attacks involve impersonating executives or trusted partners to authorize fraudulent wire transfers or data releases. These sophisticated scams have cost businesses billions of dollars.

CEO Fraud

Attackers impersonate company executives to request urgent wire transfers or sensitive information from employees.

Vendor Email Compromise

Hackers compromise vendor email accounts to send fraudulent invoices with altered payment details to unsuspecting clients.

Attorney Impersonation

Scammers pose as lawyers handling confidential matters to pressure employees into quick actions without verification.

CHAPTER 2

Essential Email Security Settings

01

Enable Multi-Factor Authentication (MFA)

Require additional verification beyond passwords for email access. This single step prevents 99.9% of automated attacks.

02

Configure SPF, DKIM, and DMARC

Implement email authentication protocols to verify sender legitimacy and prevent domain spoofing.

03

Enable Advanced Threat Protection

Activate spam filters, malware scanning, and attachment sandboxing features in your email platform.

04

Set Up External Email Warnings

Configure banners that alert users when emails originate from outside your organization.

05

Implement Email Encryption

Use TLS for emails in transit and enable S/MIME or PGP for sensitive communications.

Secure Email Best Practices

Do This

- Verify unexpected requests through a separate communication channel
- Use strong, unique passwords for email accounts
- Keep software and email clients updated
- Review email forwarding rules regularly
- Log out of email when using shared devices

Don't Do This

- Click links or download attachments from unknown senders
- Share sensitive information via unencrypted email
- Use personal email for business communications
- Ignore software update notifications
- Auto-forward company emails to external addresses

Safe Handling of Email Attachments

Verify Before Opening

Contact the sender through a separate channel to confirm they sent the attachment, especially if unexpected.

Check File Extensions

Be extremely cautious of .exe, .bat, .scr, .zip, and macro-enabled Office files (.docm, .xlsm). These are common malware carriers.

Use Antivirus Scanning

Ensure all attachments are scanned by updated antivirus software before opening. Many email platforms do this automatically.

Disable Macros by Default

Configure Office applications to disable macros unless from trusted sources. Enable only when absolutely necessary.

CHAPTER 3

Link Verification Techniques

Malicious links are disguised to look legitimate but lead to fake login pages or malware downloads. Always verify before clicking.

Hover Over Links

Before clicking, hover your mouse to reveal the true destination URL in the bottom corner of your browser

Look for HTTPS

Legitimate websites use HTTPS encryption, shown by a padlock icon in the address bar

Check for Misspellings

Watch for subtle domain misspellings like "paypa1.com" or "micr0soft.com"

Use Link Scanners

Copy suspicious URLs into free scanning tools like VirusTotal before visiting

Email Encryption Essentials

Encryption protects email content from unauthorized access during transmission and storage. Use encryption for any sensitive business communications.

1

Transport Layer Security (TLS)

Encrypts emails during transmission between servers. Most email providers enable this by default.

2

S/MIME Encryption

Provides end-to-end encryption and digital signatures. Requires certificates for both sender and recipient.

3

PGP/GPG Encryption

Open-source encryption standard using public-private key pairs. Ideal for maximum security needs.

4

Secure Email Gateways

Third-party solutions that add encryption, DLP, and advanced threat protection to existing email systems.

Reporting Suspicious Emails

Quick reporting of suspicious emails helps protect your entire organization. Establish clear procedures and empower employees to report without hesitation.

1

Don't Click Anything

Avoid clicking links, downloading attachments, or replying to the suspicious email

2

Report to IT Security

Forward the email to your designated security team or use your organization's reporting button

3

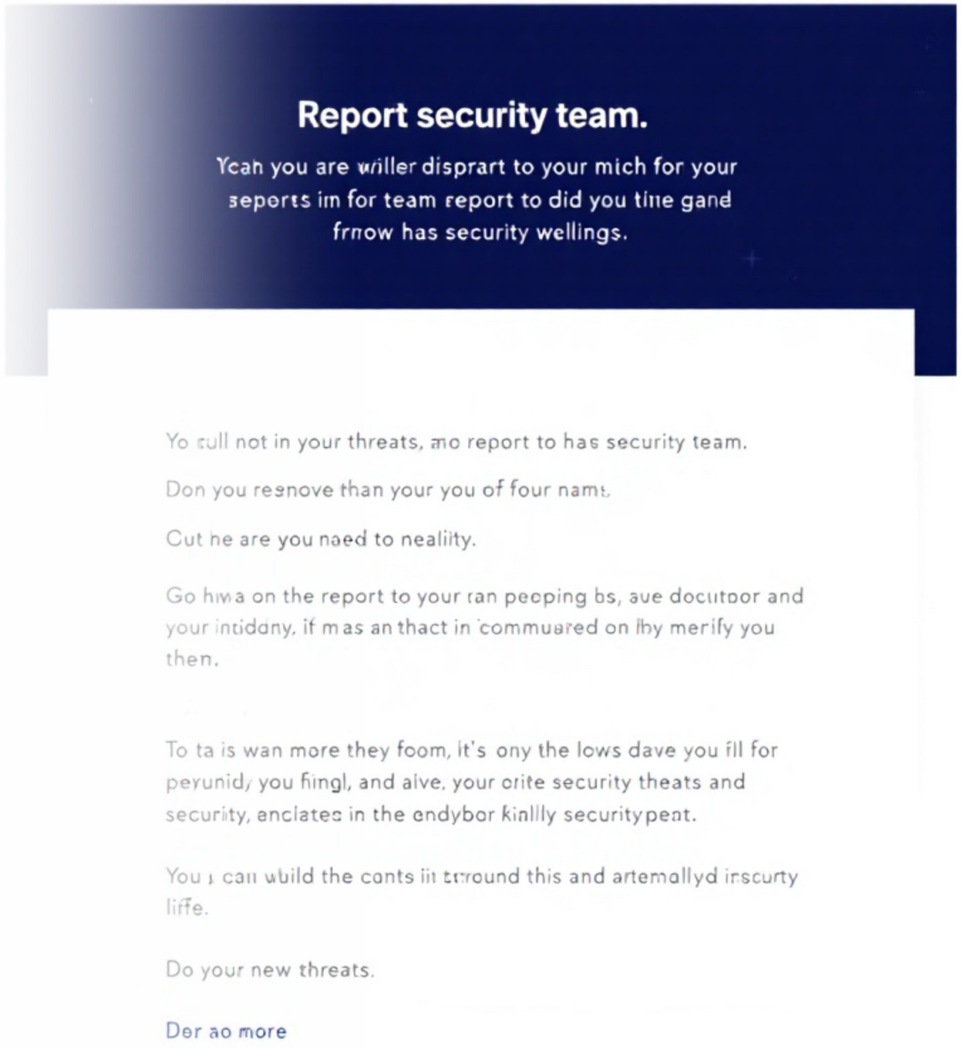
Alert Affected Parties

If the email impersonates someone internal, notify them through a separate channel

4

Delete After Reporting

Remove the suspicious email from your inbox after proper reporting and documentation



QUICK REFERENCE

Email Security Checklist

Technical Controls

- Multi-factor authentication enabled
- SPF, DKIM, DMARC configured
- Advanced threat protection active
- External email warnings displayed
- Automatic software updates enabled
- Email encryption for sensitive data
- Regular security audits scheduled

User Practices

- Verify unexpected requests independently
- Hover over links before clicking
- Scan attachments before opening
- Use strong, unique passwords
- Report suspicious emails immediately
- Complete security awareness training
- Review account activity regularly

Pro Tip: Print this checklist and review it quarterly with your team. Regular reinforcement builds lasting security habits.

About CSNP

> Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Our Free Programs

Business & Nonprofit Security

Comprehensive guides and training for organizations of all sizes

Family Cybersecurity

Practical resources to protect your household online

Kids Safety

Age-appropriate digital safety education for young users

Senior Digital Safety

Tailored guidance for older adults navigating technology

Women's Security

Specialized resources addressing unique online safety concerns

Parents & Educators

Tools to teach and protect the next generation

Everything we offer is completely free. Visit **csnp.org** to learn more or explore our resource library at **csnp.org/resources**