



Email Security Workbook

A three-phase blueprint for more effective protection against email threats.



Introduction

What if you could stop worrying about email threats without putting your business at risk?

Email is one of the most common threat vectors in the modern technology landscape, delivering everything from one-click malware to highly targeted and multi-touch social engineering attacks.



Many business owners know their email inbox can be a dangerous place, but there are a lot of misconceptions about whom it's dangerous for and how severe the consequences of not getting email security right can be.

Who Can Be a Target?

Small businesses tend to think they're small fish when it comes to cyber attacks. **Unfortunately, small businesses often find themselves as targets with 43% of attacks aimed at them each year** according to Verizon's *2020 Data Breach Investigations Report*. This becomes a self-fulfilling prophecy with small businesses failing to prioritize IT security because they don't believe they're an appealing target and hackers in turn setting their sights on these small businesses precisely because they fail to prioritize security.

A single hack into a Fortune 500 company may be more lucrative, but the low level of effort needed to breach a smaller business with no or lesser defenses in place can easily make them more appetizing targets.

For businesses who *are* concerned about security, there's another misconception that only *key individuals* are targeted. In fact, the 2020 *User Risk Report* from Proofpoint found that **60% of highly targeted phishing attacks are aimed at individual contributors and low-level management**, with only **11% aimed at executives**.

What Are the Consequences?

Attention-grabbing headlines in the IT security space often favor large attacks at well-known companies. This can lull small businesses into a false sense of security. But, email attacks on small businesses can still have cringe-worthy price tags.

Here are two attacks that happened to small municipalities in PEI's backyard (neither are PEI clients). Both attacks were sent through email and have price tags that might make you shiver. Can your business survive a \$45,000 mistake? A million-dollar mistake?

Security Intelligence
Home / News
Colorado Town Loses More Than \$1 Million to a BEC Scam
January 6, 2020 @ 12:35 PM | By David Bresson | 2 min read
A Colorado town lost more than \$1 million in a business email compromise (BEC) scam after mistakenly transferring the money to digital fraudsters.

9NEWS News Weather Sports Connect Watch
COVID-19 VACCINE CORONAVIRUS VOICES OF CHANGE NEXT WITH KYLE CLARK
CRIME
Ransomware attack forces city of Lafayette to pay hackers \$45,000
The cyberattack led to an email and phone outage at the city. There's no timeline for when that will be resolved.

The Goal for this Workbook

Unfortunately, this workbook isn't a magical roadmap to completely eliminating your risk of falling prey to email threats. **While it's always prudent to strive for 0% risk, this is not a realistic goal**—and any IT partner who promises this to you should be met with a healthy dose of suspicion.

So, while not a magical key to IT security freedom, this workbook outlines our recommended approach to tackling email security and providing adequate protection for your business.

1

Layer 1: Foundational Policy Setup and Configuration

2

Layer 2: Advanced Filtering and Protection Providers

3

Layer 3: Email Security and the Cyber Security Ecosystem

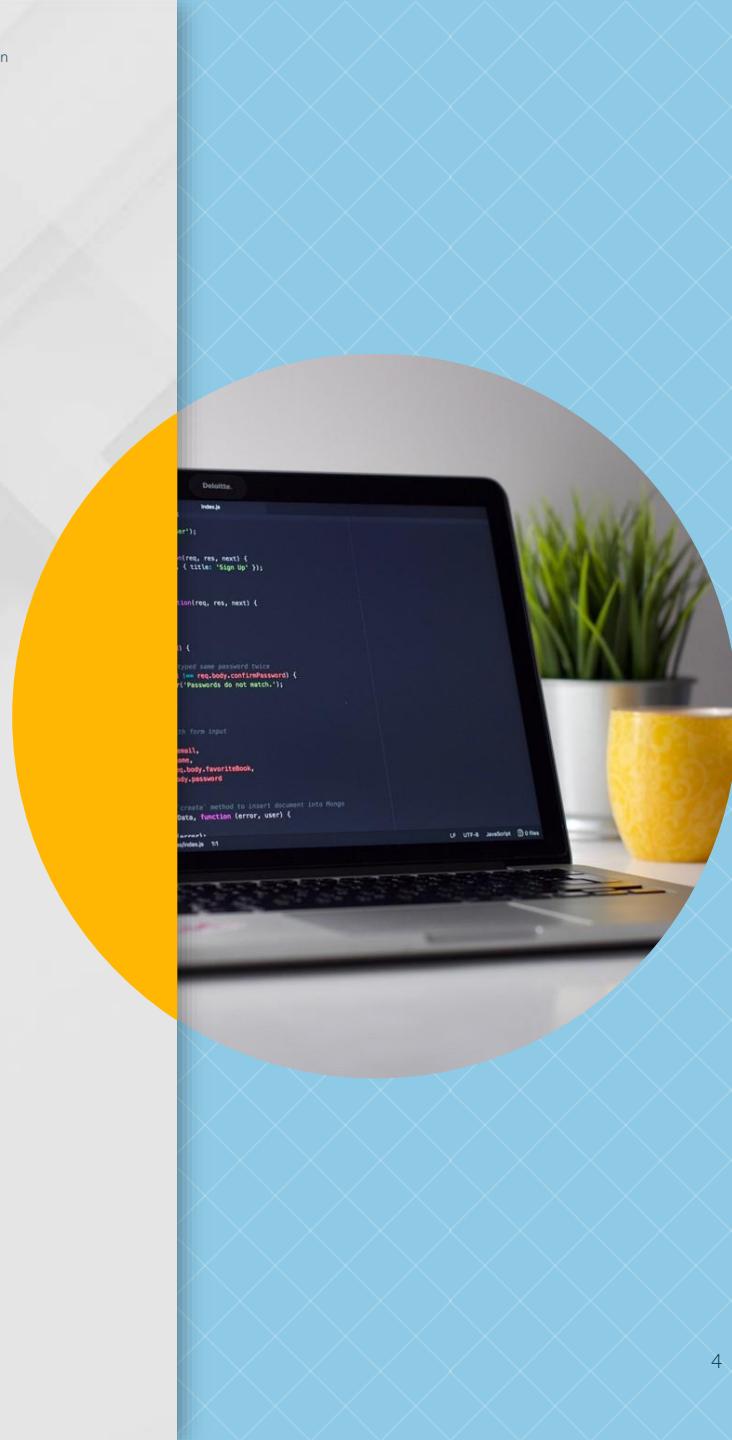


Layer One Protection: Basic Policy Configurations

Before looking for add ons or new software packages to increase your email security posture, there are a few items you can configure with your email provider immediately to increase your protection.

SPF, **DKIM**, and **DMARC** should be the first piece of your email security strategy—regardless of your email provider. They provide important authentication capabilities that ensure your email addresses can't be used against you.

For Office 365 users, **Exchange Online Protection** is included in all plans and includes basic anti-phishing, anti-spam, and other policies that can protect your business.



SPF – Sender Policy Framework

Having a properly configured SPF record can prevent spammers from sending messages on behalf of your domain. This works like the **return address** on a letter sent through the mail. If the email message wasn't sent from a server authorized in your SPF record, the email can be rejected.

Create an SPF Record

There are many SPF generators available online. These tools allow you to configure the settings for your SPF record and create the DNS record to add to the DNS Zone of your domain. We'll walk through the settings of [this generator from MXToolbox](#).

1. Fill out your domain name and click **Check SPF Record** to bring up additional settings.
2. Complete the form with the correct information for your email environment.
3. Pay special attention to the last setting, **How strict should the SPF policy be?** This is an important setting that determines how messages that fail the SPF check are handled by the receiving server:

Strict: Mail servers should always reject mail from my domain that fails the SPF check.

Neutral: Mail servers should accept and do nothing with mail from my domain that fails the SPF check (*not recommended*).

Soft Fail: Mail servers should accept mail from my domain that fails the SPF check but should send the message to the SPAM folder.

4. The SPF record will update as you fill out your required fields. Once you're happy with your configuration, click **Finalize Record**. You can now add this record to the DNS Zone of your domain.

SPF is an email authentication record that tells the receiving mail server whether email appearing to come from your domain was sent from one of your authorized mail servers.

SPF Record Generator

Domain Name or URL:

Pre-fill with record found

SPF WIZARD

Answer the questions below and we'll generate a record for you in the correct format. If you have questions, you can contact [MxToolbox Support](#)

Do you send email from your webserver?

Do you send email from the same server in your MX records?

Enter any other server hostname or domain that delivers email for your domain

Enter your domain's IPv4 Addresses / CIDR Ranges

Enter your domain's IPv6 Addresses / CIDR Ranges

Enter any 3rd party systems that may deliver emails for your domain (usually provided to you by the sending system) Ex. Google Apps, Office 365, etc.. This record is usually provided by the 3rd party.

How strict should the SPF Policy be?

Suggested Record:

```
Type: TXT
Host/Name: vandalay.it
Value: v=spf1 ~all
```

DKIM – Domain Keys Identified Mail

Having a properly configured DKIM record adds to the spoofing protections you have with your SPF record. When a mail server receives a message with your DKIM signature, it can be sure that the message is legitimate and hasn't been modified.

Get a DKIM Key

DKIM records should be generated directly from your email provider. This process will give you a public key to add to your domain's DNS records.

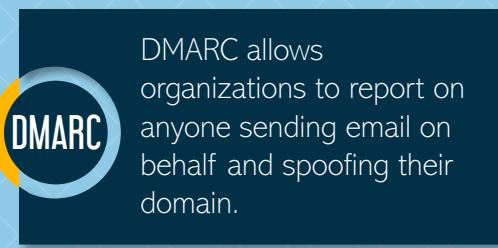
DMARC – Domain-based Message Authentication Reporting and Conformance

DMARC only works if you've set up both SPF and DKIM. All these tools work together to prevent email spoofing and make your emails more trustworthy. Once you've set up DMARC, you can get reports with detailed information on who is spoofing your domain.

Generate a DMARC Record

There are many DMARC generators available online. These tools allow you to configure the settings for your DMARC record. We'll walk through the settings of [this generator from MXToolbox](#).

1. Fill out your domain name and click **Check DMARC Record** to bring up additional settings.
2. Pay special attention to **How do you want mail that fails DMARC to be treated by the recipient?** This will determine if mail is rejected or quarantined upon failure.
3. Fill out which email addresses you'd like DMARC reports to be sent to. Use the **Show Advanced** link to further customize reports and notifications.
4. Your record will be updated dynamically as in the SPF generator. Click **Finalize Record** (not pictured) to finish. Your record can now be added to your DNS records.



DMARC Record Generator

Domain or Host Name:

HOW TO CREATE A DMARC RECORD

Answer the questions below and we'll generate a record for you in the correct format. For more details about each question or option list, click on the "Help" link beside it for more detailed information.

1. How do you want mail that fails DMARC to be treated by the recipient?
We recommend that you start with a policy of "none" - which is "Reporting Mode".
 None Help

2. What email address(es) should aggregate DMARC reports be sent to?
If adding multiple email addresses, please use a comma to separate each one.

3. What email address(es) would you like to receive forensic DMARC failure reports?
If adding multiple email addresses, please use a comma to separate each one.

Would you like to have MxToolbox automatically process your DMARC reports for analysis and delivery insights?
 Yes Help

Exchange Online Protection (EOP)

If you host your email through Office 365, you already have access to Exchange Online Protection at no extra charge. We recommend visiting EOP in the admin center to ensure the default policies are enabled for your business. You can access Exchange Online Protection by navigating to protection.office.com/threatpolicy

Enabling and Customizing EOP Policies

There are three available policies, and we recommend you turn on and customize each (where possible) for your business: anti-phishing, anti-spam, and anti-malware.

Anti-Phishing:

Without more advanced packages from Office 365, you can only enable the default policy for Anti-Phishing.

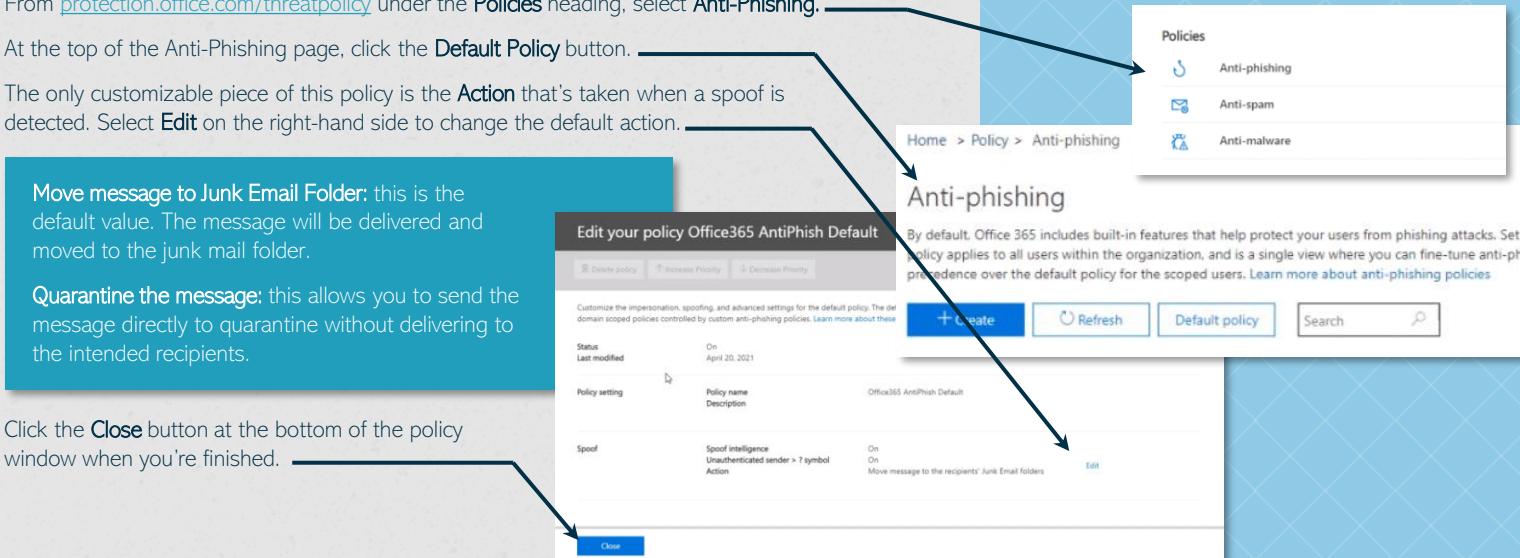
- From protection.office.com/threatpolicy under the **Policies** heading, select **Anti-Phishing**.
- At the top of the Anti-Phishing page, click the **Default Policy** button.
- The only customizable piece of this policy is the **Action** that's taken when a spoof is detected. Select **Edit** on the right-hand side to change the default action.

Move message to Junk Email Folder: this is the default value. The message will be delivered and moved to the junk mail folder.

Quarantine the message: this allows you to send the message directly to quarantine without delivering to the intended recipients.

- Click the **Close** button at the bottom of the policy window when you're finished.

- 1 Anti-Phishing: protect users from phishing attacks and configure safety tips on suspicious messages.
- 2 Anti-Spam: protect your organization's email from spam, including what actions to take if spam is detected.
- 3 Anti-Malware: protect your org's email from malware, including what actions to take and who to notify if malware is detected.



Exchange Online Protection (EOP)

Anti-Spam:

Anti-Spam comes with four policies by default that you can edit: default spam, connection filter, outbound spam filter, and spoof intelligence.

1. From protection.office.com/threatpolicy under the Policies heading, select Anti-Spam.
2. Click the drop-down icon to the left of the policy you want to edit.
3. Click the **Edit Policy** button to make changes to this policy.

We recommend turning on **Safety Tips**, **Zero-Hour Auto Purge**, and **International Spam** in the Default Spam Policy:

Safety Tips: Display safety tips from Microsoft inside users' inboxes when a message is suspected as spam. For example, "This message originated from outside your organization."

Zero-Hour Auto Purge: Protect your mailbox from new and emerging threats retroactively as they're detected, even if they've already been delivered.

International Spam: Automatically send messages to spam based on their language or country of origin.

Name	On	Type	Priority
Default spam filter policy (always ON)	On		Lowest
Connection filter policy (always ON)	On		Lowest
Outbound spam filter policy (always ON)	On		Lowest
Spoof intelligence policy (always ON)	On		Lowest

Default spam filter policy (always ON)

Edit policy

Relative priority: Lowest

Summary

- Detection response for spam: Move message to Junk Email folder
- Detection response for high confidence spam: Move message to Junk Email folder
- Mark bulk email as spam: On
- Threshold: 7
- Sender block list: Not configured

Domain block list: Not configured
Sender allow list: Not configured
Domain allow list: Not configured
International spam - languages: Off
International spam - regions: Off
End-user spam notifications: Off
Configure end-user spam notifications...

Anti-Malware:

Anti-Malware only comes with one default policy, but it has several customizable features.

1. From protection.office.com/threatpolicy under the Policies heading, select Anti-Malware.
2. Hover over the policy and select the checkbox to the left of the policy name.
3. Click the **Edit Policy** button on the policy pane to make changes to this policy.

Name	Priority	Status
Default	Lowest	Off

Default

Edit policy

State: Enabled

Malware Detection Response: notify users if one of their messages is quarantined for malware with a default or custom message.

Common Attachment Types: off by default. We advise turning it on to specify file types that should always trigger the malware response.

Malware Zero-Hour Auto Purge: retroactively detect and neutralize malware that has already been delivered to user inboxes.

Notifications: determine if senders or administrators should be notified about detected malware. Customize the response or use the default.

Layer Two Protection: Advanced Filtering Packages

If you're on a mission to reduce email risk, you'll want more filtering and protection capabilities than are available in any "default" package.

Your choice for more advanced providers is going to depend on vendor compatibility, pricing model, and customization level, but we recommend finding a package with [Link Protection](#); [Attachment Protection](#); and [Advanced Anti-Phishing](#), [Anti-Spoofing](#), [Anti-Spam](#), and [Anti-Malware](#) policies.

Stick around to learn about how these features work and some of our preferred providers. You can work with PEI on any of these solutions to [simplify installation and management](#).

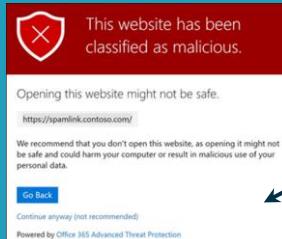


Advanced Filtering and Protection Capabilities



Advanced Link Protection

URL scanning as messages come in to identify malicious websites. Rewriting of links in inbound mail and time-of-click verification of URLs and links in email messages.



Re-written links open first to the provider for verification that they're not malicious. Once they're determined to be safe, the user is redirected to the original URL.

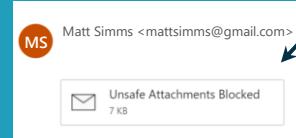
Malicious links are blocked with users sent to a notification page.



Advanced Attachment Protection

Attachment scanning as messages come in to identify malicious files. Protection against file types that are uncommon for your domain.

Attachments are opened and tested for malware in a virtual environment called a sandbox before they're delivered to recipients.



Files can be converted to a safe format or completely deleted if necessary.



Advanced Anti-Phishing, Anti-Spoofing, Anti-Malware, and Anti-Spam Capabilities

On top of the protection offered by your provider's default policies, you should look for the ability to create custom policies, fine-tune sensitivity thresholds, and analyze attack patterns across inboxes to identify coordinated attacks.

Pro Tip: Before you pull out your wallet, you may already have some of these capabilities.

Microsoft Defender for Office 365 (previously Office 365 Advanced threat Protection) is one popular solution for businesses using Office 365 as their mail provider. Defender for Office 365 Plan 1 is included in Microsoft 365 Business Premium, and Plan 2 is included in the Office 365 E5, Office 365 A5, and Microsoft 365 E5 plans. It can also be purchased as an add on for other Office 365 or Microsoft 365 plans.

[Plan 1 vs. Plan 2 Comparison](#) | [Safe Links](#) | [Safe Attachments](#) | [Configure Anti-Phishing Policies](#) | [Anti-Malware Policies](#) | [Anti-Spam Policies](#)

Choosing an Email Security Provider

There are hundreds of email security solutions on the market, and your decision on a provider should take into account the specific needs of your business.

When choosing whether to go with a third-party solution or a more advanced package from your email provider, there are two main schools of thought:

- Choosing a third-party vendor can provide better protection because it **delivers an outside perspective** on important threats and capabilities that your mail provider may have missed.
- Selecting an advanced package from your existing mail provider, for example Defender for Office 365 from Microsoft, **prevents having a siloed or fractured security environment** with too many vendors that can be more difficult to manage.

PEI's Recommended Email Security Providers (in no particular order)



Strengths:

If you're on Office 365, keeping everything under one roof avoids security silos.

Defender for Office 365 may already be included in your plan.

Access to advanced and custom policies backed by Microsoft.

Trade-Offs:

Can be complex to manage and fine-tune.



Strengths:

Third-party solution adds a fresh perspective to validate and add to existing security strategy.

Extremely customizable with nearly limitless possibilities for custom policies.

Trade-Offs:

More advanced installation and management.



Strengths:

Third-party solution adds a fresh perspective to validate and add to existing security strategy.

Simpler installation, set up, and management.

Trade-Offs:

Not a lot of custom troubleshooting or policies

Pro Tip:

Working with an experienced IT partner like PEI can streamline the installation and management process for these solutions, allowing you to take advantage of more advanced and highly customizable products without being afraid of the extra work that goes into building and configuring the unique policies needed by your business.

PEI is a Microsoft, Mimecast, and Proofpoint partner. Work with us to get the same licensing at or below MSRP with the added benefit of having an experienced partner to guide the way.

Layer Three Protection: Your Cyber Security Ecosystem

Cyber security is an ecosystem, not a series of silos. In the modern threat landscape, it's not enough to secure each aspect of your business with a separate solution and strategy. Instead, your **security practice should consist of overlapping and interwoven elements** that work in harmony to provide protection for your business.

We recommend these three practices that complement your email security posture: **multi-factor authentication**, **regular end-user awareness training**, and **backups**.



Multi-Factor Authentication (MFA)

Microsoft and Google made [headlines in 2019 when both publicly stated](#) that multi-factor authentication was the single most effective protection against account breaches, [stopping 99.9% of attacks](#).

We're not going to weigh in on the Microsoft vs. Google debate, but [when both Google and Microsoft recommend the same thing, it's probably a good time to start following their advice](#).

How this Increases Email Security

In cases where users are tricked by phishing messages into handing over their username and password, hackers won't be able to access the account without successfully passing the MFA prompt.

If your users receive an MFA prompt for a login request they didn't initiate, [they should reset their password immediately](#) to keep their account safe.

All Your Accounts Need MFA

One common misconception around MFA is that you only need to turn it on for admin accounts. While some employees may not have IT admin access, it's still important to protect those accounts with multifactor authentication. [Hackers can use these lower-ranking accounts to make future attacks more successful](#).

1

Step 01: Your receptionist's account credentials are compromised with a phishing email.

2

Step 02: The hacker accesses your global address list to determine which users to target next.

3

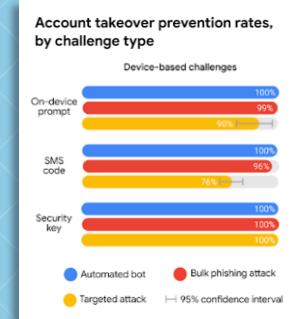
Step 03: The hacker targets your IT admin with an email from the receptionist's account.

Microsoft: Using multi-factor authentication blocks 99.9% of account hacks

Microsoft cloud services are seeing 300 million fraudulent sign-in attempts every day. MFA can help protect accounts against many types of account takeover attacks.

New research: How effective is basic account hygiene at preventing hijacking

On-device prompts, a more secure replacement for SMS, helped prevent 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks.



End-User Training and Attack Simulation

If you were paying attention in the introduction—and no harm if you didn't, because we're about to tell you again anyways—you know that email attacks aren't just hitting your "most important" or "highest access" users. **Attackers are targeting every user at your business**, and they just need one small mistake to get a foothold in your environment. This, coupled with the fact that attacks are constantly evolving, means that **ongoing end-user training is a must for keeping your business protected**.

With an attack simulator, you can put your users' knowledge to the test. Send your users simulated email threats, track who is clicking on them—or worse, handing over their credentials—and automatically assign training to users who need a little more help.

Over time, you should **see the number of users who fail these tests decrease** as they learn to approach their inbox with a more discerning eye. We recommend sending out a simulation once a quarter to keep users on their toes without overwhelming them.

Be Tactful with User Remediation

It's important to remember that while users can be your weakest security link, they're also **one of your organization's biggest assets**. Don't approach users who fail phishing tests with threats or shame. The tone you set in your response will go a long way toward helping users change their behavior.



Step One: Simulation

Send a simulation email to your users after you've provided training.



Step Two: User Action

Track if they click on or provide credentials for the attack.



Step Three: Training

Show users right away what they missed and assign further training.



Pro Tip:

Before you do any simulated attacks, provide training for your users. *The goal is not to trick people but educate them.*

Test your users on each of these common types email threats so they're familiar and easy to recognize:

Social Engineering Attacks: attempts to deceive users into divulging sensitive information.

Suspicious Emails: internal or external messages from scammers.

Malicious Links: links to spoofed websites.

Infected Attachments: emailed files with malware in the macros.

Malvertising: advertisements that send users to malicious sites or that are infected with malicious code.

Vishing: emails with fake voicemail attachments containing malware or a malicious link to an online voicemail portal.

Rinse and Repeat

Repeat this process a few times each year, even for users who successfully pass your simulated attacks to keep your users vigilant and introduce them to new types of threats.

Data Backup

There's no such thing as 0% risk. While you can't prepare for *every* possible situation, you *can* have a backup plan.

One common objection we hear against having a solid backup plan in place is, "My email and files are in Office 365, doesn't Microsoft back it up for me? They told me my data is replicated 6 times over!"

Unfortunately, it's **another pesky misconception that data replication is the same thing as having a backup**. It is true that your data in Office 365 is replicated all around the U.S. But, if one of your users becomes infected with malware they download from a malicious email, you run the risk of that virus being replicated as well, infecting all the copies. If this happens, there's no easy way to reverse the encryption on those files.

Prepare for the Worst

Keep periodic backups of your employees' mailboxes and files. Depending on how often you run these backups, you may be restoring data from a slightly outdated copy, but at least you've got something to restore.



It's a pesky misconception that data replication is the same thing as data backup.

Conclusion

Ready to dive in? There's no one-size-fits-all strategy for email security, and you should always prioritize the specific needs of your business.

But, as you move through the three layers of protection and lay the groundwork, you're well on your way to better protection for your users, your data, and your business.

Get in touch to learn how PEI can help you [make your technology a business advantage](#).

Need Help?

PEI has over 30 years of experience deploying advanced engineering solutions centered on security, collaboration, cloud computing, networking, and technology management. We work with small and midsize businesses, helping them use technology to meet their business goals and solve their business problems.

If you need help building an email security strategy that works for your business, our experienced experts are ready with a [free email security assessment](#), where we'll identify your unique risk factors and [build a custom plan for protecting your business against threats](#).



Get Started
303-786-7474 | info@pei.com | www.pei.com