Lure Out the Phish:
Email Security Best Practices

Your email security system's filter might be firing on all cylinders, but it's still possible for a cleverly crafted fake email, or an email from a compromised trusted sender, to get through to your users. Your email safety training is critical to averting what can be a devasting financial (or reputational) loss.

It's all about the money

According to the 2021 Internet Crime Center Report, during the year there were 19,954 business email compromises. Altogether, they incurred a total of $2.4 billion in losses.

Deer Brook's team has assisted with countless fraud cases where a phishing scheme led to compromised bank accounts, fraudulent wire transfers, and misdirected contractor payments. If we tally the losses over the years, it's in the millions of dollars.

Always question unexpected emails

A phone call can do so much.

If you receive an unexpected email with a link or attachment from a trusted sender, call them to verify they sent it. Don't ask them through email, because their email account is likely already compromised.

Test your users with phishing simulations

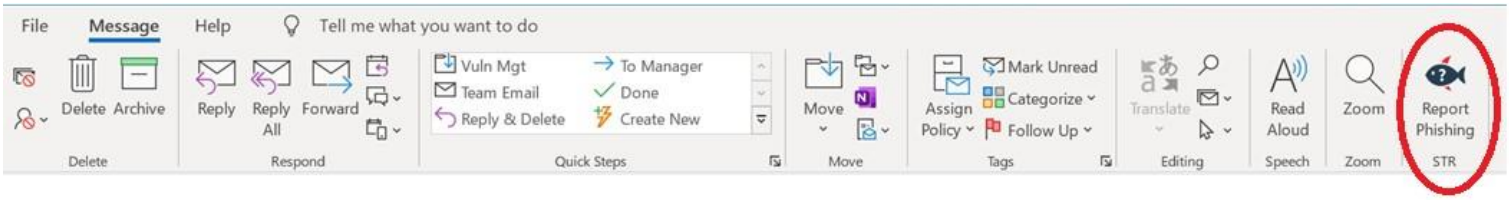
Users need to be periodically tested to reinforce the training they receive. The best way to test is by subscribing to a commercial phishing test and training solution. There are several on the market, but Deer Brook recommends KnowBe4.com or Cofense.com. Key elements to look for are:

- A scheduler so you can set up tests in advance, and even stagger tests within the test period.
- A catalog of phishing email topics so you can mix them up and not send the same ones to your users.
- The ability to send different kinds of emails out during the same test, so users are less likely to tip each other off if they guessed the phishing emails are a test.
- Automated enrollment to online training for users who fail a phishing test, and a notification to someone if they do not take the training.

- Key performance indicators for phishing test fail percentiles that you can include in your security metrics.
- Tracking of users who fail tests, so you can tailor your in-person coaching.

Add a report button to your users' Outlook app

Give your users the ability to easily forward questionable email to your Information Security team. Let the experts on your IS team diagnose the email.



Both Cofense.com and KnowBe4.com offer a *"Report Suspicious Email"* Outlook addon that forwards questionable email to your security team.

Your team can determine authenticity and let the user know if the email is safe, marketing junk, or a phishing attack. Deer Brook has found this to be a powerful tool in stopping phish emails.

Note: *Microsoft offers an addon as well, but it sends the email to themselves to check for malware and does not return the email to you if it is safe. Instead, it serves as a tuning process for their anti-phishing filter.*

Things to avoid

- Don't exclude anyone from your safe email handling training and testing. We often see executives excluded so that they won't be embarrassed if they fail the tests. Alternatively, the thought may be that they're busy folks and don't have time for such training. However, that couldn't be further from the truth. Executives are the most likely users to be targeted by phishing crooks. Executives have access to sensitive information, large sums of corporate funds and have the authority to influence staff. You may not

want to publish their names, but if they do happen to fail tests, it will be a good catch that you can discuss in private.

- Don't push your test schedule out too far. Deer Brook recommends a monthly test to keep users on their game. Monthly test results provide a very valuable security metric for metric scorecards.
- Everybody gets one; folks are going to fail a test or two. Many of the test scenarios can be very sophisticated. Deer Brook recommends you provide in-person coaching to anyone who fails two times or more in a year, to be sure they have responsibility and know the processes to safely handle email.
- Don't take poor results personally. Unfortunately, you may have a user that continually fails phishing tests, and it can be evident that they are a business risk. Sometimes tough decisions have to be made on whether someone should have access to external email or be in any position of trust if they cannot handle email prudently.

To gamify or not to gamify

You can take your training and testing to the next level with phishing derbies.

With Outlook's *"Report Phish"* button, users can report suspicious email and you could offer an award or gift card to users who report verified phishing emails. These programs are typically low budget, and can be managed without much effort.

As you consider creating a phishing reporting program, keep in mind that as is the case with most things, there are pros and cons to a gamified email security program.

To Gamify (Pros):

- Provides an incentive to catch phishing emails
- Maintains email security mindfulness
- Rewards good habits

Not to Gamify (Cons):

- Many users will never receive an actual phishing email, and over time they may not care to participate if they sent in a test email or marketing email and never received an award.

Wrapping up

Deer Brook's experts are here to help you with strengthening your email security program: whether you need a review of your email security solution, training, and testing, or you want to outsource training and testing to us.

We also provide cybersecurity incident response that includes business email compromise response; we are here to help.

deer-brook.com

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS