LEFT OF BREACH

2018

COFENSE.COM

INTRODUCTION: WANT TO STAY IN FRONT OF BREACHES? TRAIN LIKE THE MARINES.

Too often in cyber security, people focus on mitigating breaches after they occur—and long after phishing emails deliver malicious payloads. To lower the threat, many companies now train employees by sending them simulated phishes, so they can learn to recognize and report suspicious messages.

It's the kind of proactive thinking the Marines call "left of bang."[1]
In the security world, it's more like left of breach.

The Marines Combat Hunter training works on this premise: by understanding what "normal" looks like, we're much more likely to recognize activities and behaviors that are out of place. That recognition, even if based on "gut feel," becomes the trigger for acting.

This approach relies heavily on front-line human assets, not just technology, to detect attacks in progress. Most important, it lets you get ahead of trouble before it blows up.

Following are 3 ways to apply this thinking to your phishing defense.

1."Left of Bang: How the Marine Corps' Combat Hunter Program Can Save Your Life," Patrick Van Horne and Jason A. Riley, Black Irish Entertainment LLC, 2014.

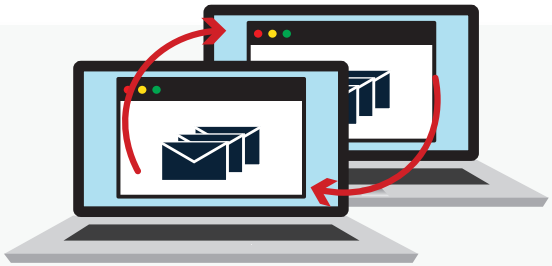
1. **BASELINE** YOUR COMPANY'S WEAKNESS

Hey, the bad guys do. Threat actors begin by identifying your weak spots so they can exploit them. Get on the same page. Do a thorough analysis of your security environment, business operations, active threats and employee engagement. All of this will inform your phishing simulations.

It's smart to do a **"what's normal?"** checklist.

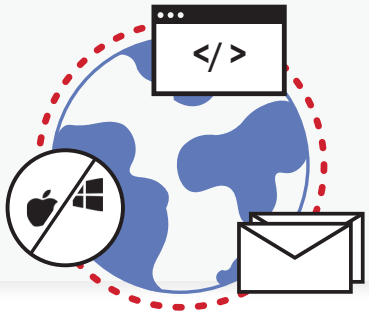
So, what are some typical questions to ask yourself?

THE SECURITY ENVIRONMENT



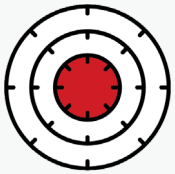
What are normal traffic flows and email patterns?

Where does your most critical data reside and who has access?

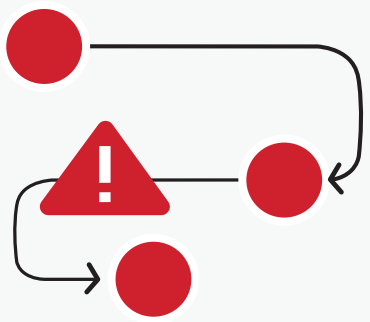


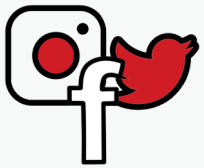
And what operating systems, email clients and browsers are you using?

BUSINESS OPERATIONS

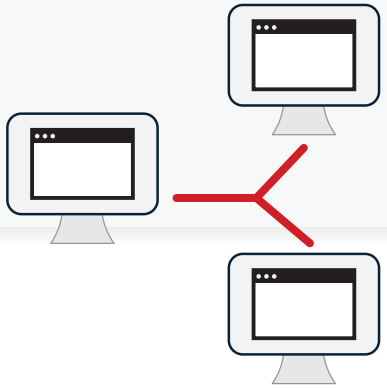


- Who are my highly visible, high-authority targets?
- What are my highest risk business processes? (e.g. sending PII attachments in email)

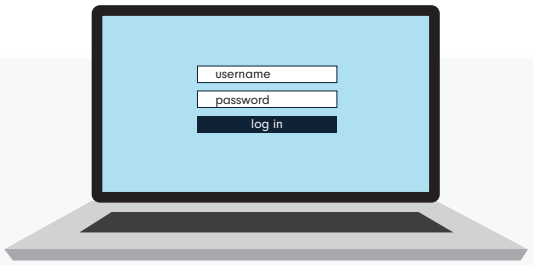


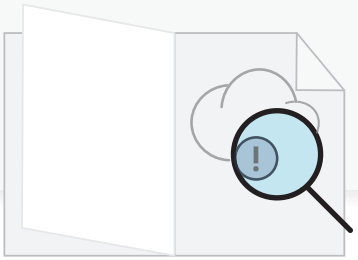


- What social media platforms do we use and what information are we sharing publicly?
- How many third-party vendors access my network or interact with us via email?



ACTIVE THREATS





- What phishing campaigns are we being hit with today?
- How is our industry being targeted by malicious actors?
- Do we understand our risk exposure to current attack models?

EMPLOYEE ENGAGEMENT

Do our employees view themselves as responsible for information security?

Have we shown our users how to identify a phish?

Have we empowered our users to report suspicious activity for analysis and response?

You'll probably have your own questions to add to this list. Once you've gathered the answers you need, you're ready for **step 2**.

2. DESIGN PHISHING SIMULATIONS THAT LOOK LIKE **THREATS YOU FACE**.

Now you can phish your employees. Your checklist has yielded the baseline information to simulate phishes. Again, be sure to incorporate what you know about active phishing threats. By understanding current or trending threats, you'll develop simulations that mirror real attacks and get results that show your risk exposure.

After announcing the training program so employees know what to expect—including the message that simulations are meant to educate, not berate—start sending mock phishes ranging from basic to more advanced.

Over 12 months, you might for example send:

An innocent looking e-greeting card

An invoice attachment that really isn't

A social media invitation to disaster

And a request for funds, seemingly from a trusted source but in fact a form of social engineering known as business email compromise (BEC)

It's really, really important to deliver simulations to everyone. The C-level gets phished all the time. So do HR and finance. And oh yes, IT.

You'll also want to do follow-up simulations based on what you've learned from the first few rounds. Over time, as employees get better at catching basic phishing tactics, you'll probably decide to mix in some more advanced scenarios—again, based on real threats your incident responders see.

NEED HELP? TRY COFENSE PHISHME™

It's the industry-leading solution for running phishing simulations. Thousands of companies use it, including much of the Fortune 1000. Demo it live now!

3. TRAIN **EVERYONE** TO REPORT PHISHING.

Recognizing a phish is good. Reporting it is better. When you train your people, all of them, to report suspected phishing they become human sensors, so to speak, and help shorten your meantime both to detection and response.

Many organizations have installed simple reporting plugins to their email toolbars. With one click, employees can send potential phishes to the security team for quick analysis and, if needed, incident response.

It's the sort of thing that helps to keep your business left of breach—taking proactive steps instead of accepting that the bad guys will succeed.

COFENSE REPORTER™

Give them something good to click.

People love to click. So, let your employees click on something helpful rather than a phishing email. Cofense Reporter is a button that lives in your email toolbar. One click sends suspicious emails to your help desk or IR team, giving them human-vetted intelligence to:

Detect and respond to phishing faster

Use third-party integrations to analyze URL and malware attachments

Prevent or minimize breaches

According to Cofense's latest Phishing Resiliency and Defense Report, reporting comes with an added benefit. It not only notifies your security teams of possible attacks, it actually drives down your phishing susceptibility rate. How's that? Well, engaged employees are vigilant employees, on the front end as well as the back end. Giving users the satisfaction of doing something about the problem makes them more likely to identify the problem in the first place.

LET'S REVIEW

To build a better phishing defense:

1. Baseline your company's weaknesses, so you know where to focus your efforts.
2. Design simulations that mirror real threats your IR team sees.
3. Condition the entire organization to report phishing.

Cover all 3 and you'll better your odds of staying left of breach. Kinda, sorta like the Marines. **Boo-rah!**

Learn more about phishing defense:

Read Cofense's latest Phishing Defense and Resiliency Report.