# HOW TO TRAIN YOUR CYBERCRIMINAL

## Learn the signs of a phishing attempt and what to do next


## THIS MONTH'S TOPICS:

**Curiosity Killed the Cat**

*Social engineering at its finest...*

**Have a Bone to Pick?**

*How to report a scam attempt...*

**Scam of the Month:**

Adopting a criminal...

**Cyber Zen Den:**

*Cat & Dog...*

The month of August is home to International Cat Day (August 8th) and International Dog Day (August 26th).

To honor our furry friends, this month's newsletter has all the best pet puns that a cyber cat could ask for!

With the average employee receiving 121 business related emails per day, it can feel like a lot of pressure to catch a phish, but with some cat-like reflexes, and a few of these cybersecurity best-practices, you'll be able to put a muzzle on that next scam attempt.

# CURIOSITY KILLED THE CAT

**A TAIL OF SOCIAL ENGINEERING**

We know social engineering as the psychological manipulation of users to trick them into divulging information or performing actions they would not otherwise.

Curiosity is one of the many social engineering techniques that just might get you every time!

## LOOK OUT FOR

- **BAITING:**
  Enticing ads, links or attachments that pique your interest enough to click without due diligence.
- **SCAREWARE:**
  False alarms that prompt you to install software in order to fight fictitious malware.
- **PRETEXTING:**
  Scam messaging, sometimes impersonating someone you know, requesting certain information from you in order to confirm your identity.

## DON'T BE TEMPTED BY

- Emails from suspicious sources
- Too-good-to-be-true offers

# Have a Bone to Pick?

## HOW TO REPORT A SCAM ATTEMPT

## Inform your supervisor

If you catch a phish at work, informing your supervisor can be an important step in stopping the spread of the scam.

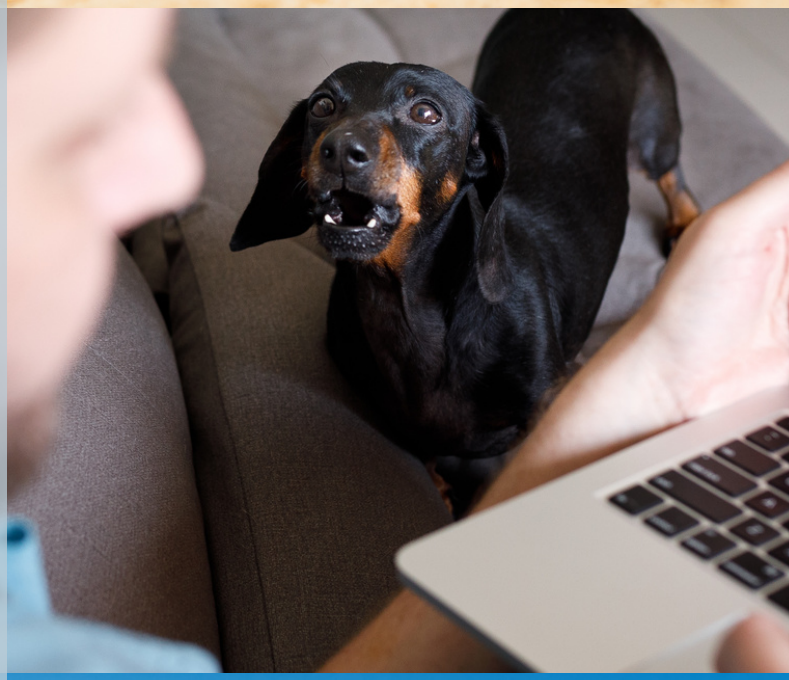
By making your supervisor aware of the situation, they can provide you with the company's next steps, and alert the team so that no one else gets hooked.

Note what the scam entailed, and the address it supposedly came from, but do not forward the email, as this may increase the likelihood of the malicious link or attachment being clicked.

## Tell IT

If you think you've caught a work phish, but you're not entirely sure, some company's have a "phish tank" where you can forward suspicious emails to IT for further analysis before interacting with them.

If you think you've caught a phish, or are just unsure, and have already informed your supervisor, they may advise you to update IT, as well. By keeping IT in the loop, their department can send out appropriate alerts to the company and help contain any potential threats.



## Inform others

Finding a phishing attempt in your personal inbox may feel a bit more threatening, as it can come across as a personal attack, but know that you're not alone. Government agencies have online forms that you can fill out to report your scam, and help fight fraud overall.

Sharing your experience with phishing attempts with friends and family can also help spread the word about currently circulating scams so that your loved ones don't get caught next.

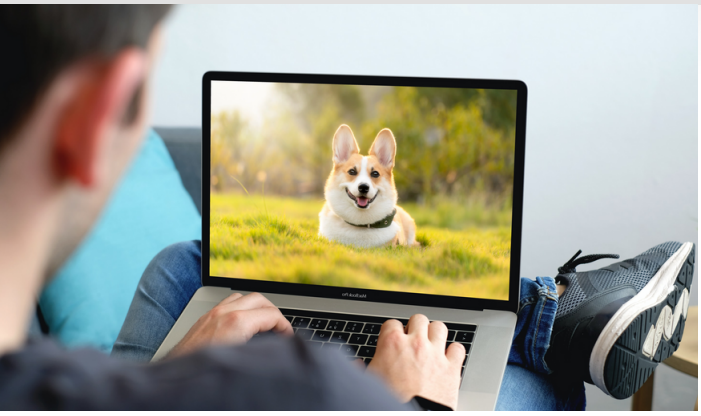
# SCAM OF THE MONTH

*Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.*


Walter has always wanted a dog, and now that his new job lets him work from home,  it is the perfect time to find a furry friend.

He started searching online and found one woman who was moving to a new apartment that didn't allow pets. She was hoping to re-home her pup as soon as possible so that he would not have to go to a shelter.

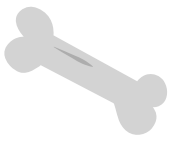
The ad did not include much information about the dog, but Walter didn't think anything of it because the pictures were so cute. He reached out to the woman to express his interest in adopting the pet, and even offered her references. She never asked any questions of him, but did request that he pay a "holding fee" and cover the charges to ship the animal from her location. Walter asked if he could just go pick up the dog so that they could meet in person, but the owner refused claiming she was too busy with the move.



## Did you spot the red flags?

- Rehoming ads that do not include information on the pet, their personality, or health information can be a cause for concern.
- A legitimate rehoming often involves the owner asking questions of the adopter, or includes an adoption application.
- Limiting in-person contact by not allowing a meet-and-greet is often a bad sign that the animal does not exist.

One common pet adoption scam requires the adopter to pay for the "shipping cost" of the animal. The adopter is sent to a fraudulent website to input their information. The money is taken from their card, but the animal never arrives.



Another way that scammers can easily steal money from potential adopters is by requiring a deposit to "reserve" the animal. Keep an eye out for suspicious forms of payment, as well, such as cash, wire transfer, or gift cards.

Many classified / advertising websites ban the sale of animals, however, sellers can often skirt these rules by using the term "rehoming." The easiest way to avoid pet adoption scams and stop the use of online forums to buy and sell animals, is to adopt from a reputable animal rescue / organization or from your local animal shelter.


## Key Takeaways

With a dose of due diligence, and a smidge of best practices, anyone can learn to train their cybercriminal.

Knowing what to look out for, and who to inform should you catch a phish is all you need to make your inbox a "good boy!"

**That's curious:** Curiosity often gets the best of us, especially in a scam. But understanding that scammers are trying to use our curiosity against us can help you spot a social engineering tactic next time you see one.

**Sharing is caring:** When a scam finds its way into an inbox, most people delete it and move on. But by sharing what you've received, and spreading the word of your experience, you can help protect others from making a dire mistake.

**Man's best friend:** Pets are too cute to question, which is why cybercriminals take advantage of that adorable ball of fluff for their own scamming purposes. Don't let the excitement of adopting a new friend get in the way of your cyber vigilance.

# Cat & Dog

Cat and dog is a yoga stretch. By simply getting on all fours and lifting your head and dropping your belly (for cat), or releasing your head towards the floor and curling your back up (for dog) you can increase spine mobility and improve balance.

### How does this relate to cybersecurity?

Think of cybersecurity awareness as your "spine's mobility." The more you learn about what types of scams are out there, and how to avoid them, the more you will be able to move about the internet with ease, and the better you will be able to "bounce back" should a scam attempt to trip you up.

### Now apply this concept to cyber-awareness.

Connect with your supervisor or a colleague and ask them what phishing scam attempts they've received or heard about in the office. Then challenge them to forward the question on to someone. This will help open up dialog about scams, and keep everyone up to date on what types of scams seems to be circulating within your industry.