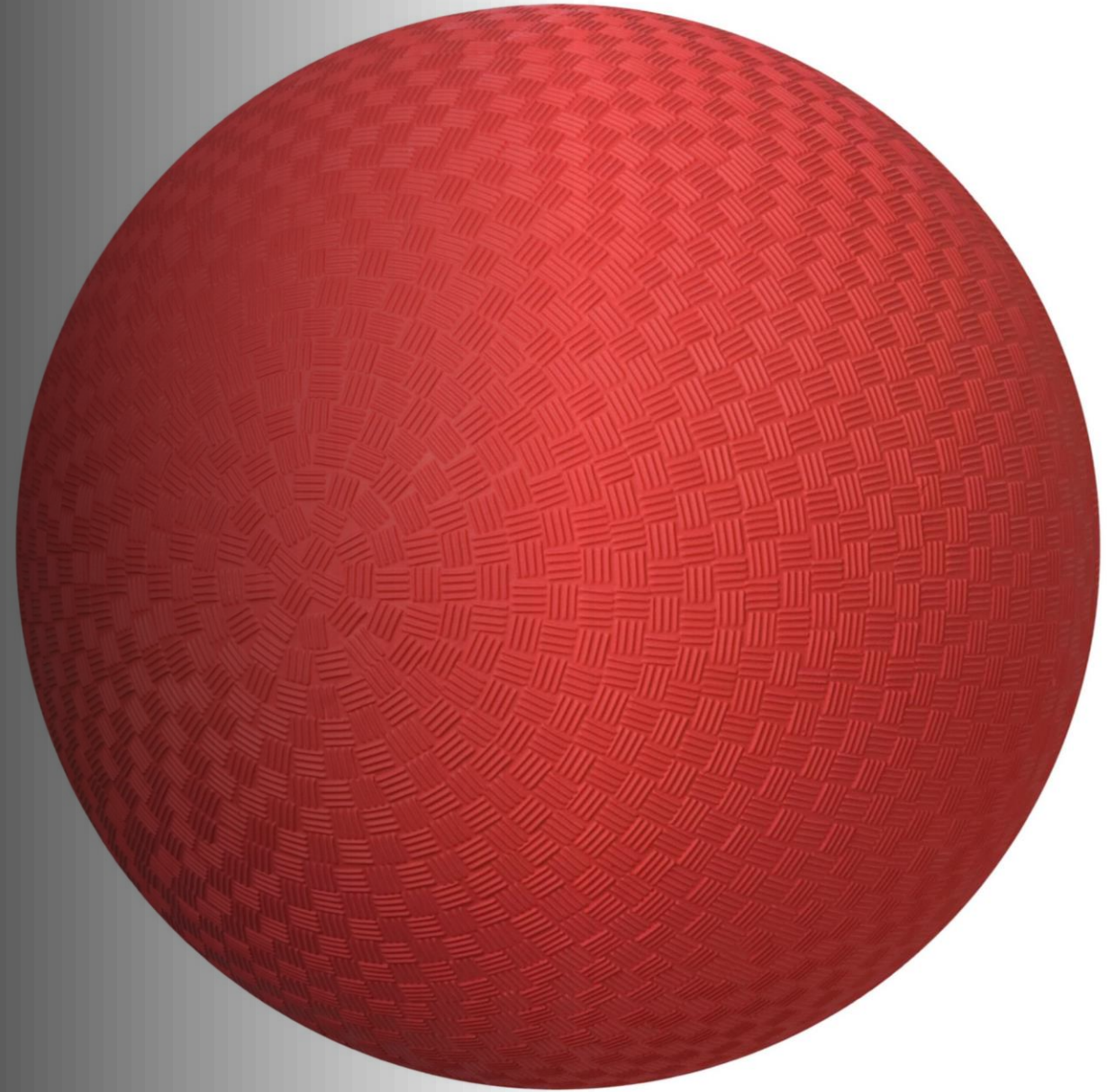




# CYBERSECURITY: Everyone can do it.

---

Nathan Abbott, CISA, CFE, EA  
Information Systems Audit Manager





# DISCLAIMER


- ***The Opinions expressed during this presentation are my own. They do not necessarily represent the views of the Tennessee Comptroller of the Treasury, his representatives, or the Tennessee Department of Audit.***



CYBERSECURITY:  
Everyone can do  
it.

---

Nathan Abbott, CISA, CFE, EA  
Information Systems Audit Manager



**IF YOU CAN  
CLICK ON AN  
EMAIL, YOU  
CAN CHANGE  
A PASSWORD**

# Five's "P" of Cybersecurity

- **PEOPLE**

- **PHISHING**

- **PASSWORD**

- **PEOPLE**

- **PATCHES**





PEOPLE

YOU ARE THE FIRST LINE OF DEFENSE.



# PASSWORDS

- Strong passwords
- Don't re-use passwords
- Change passwords
- Add Multi-Factor Authentication



# STRONG PASSWORDS

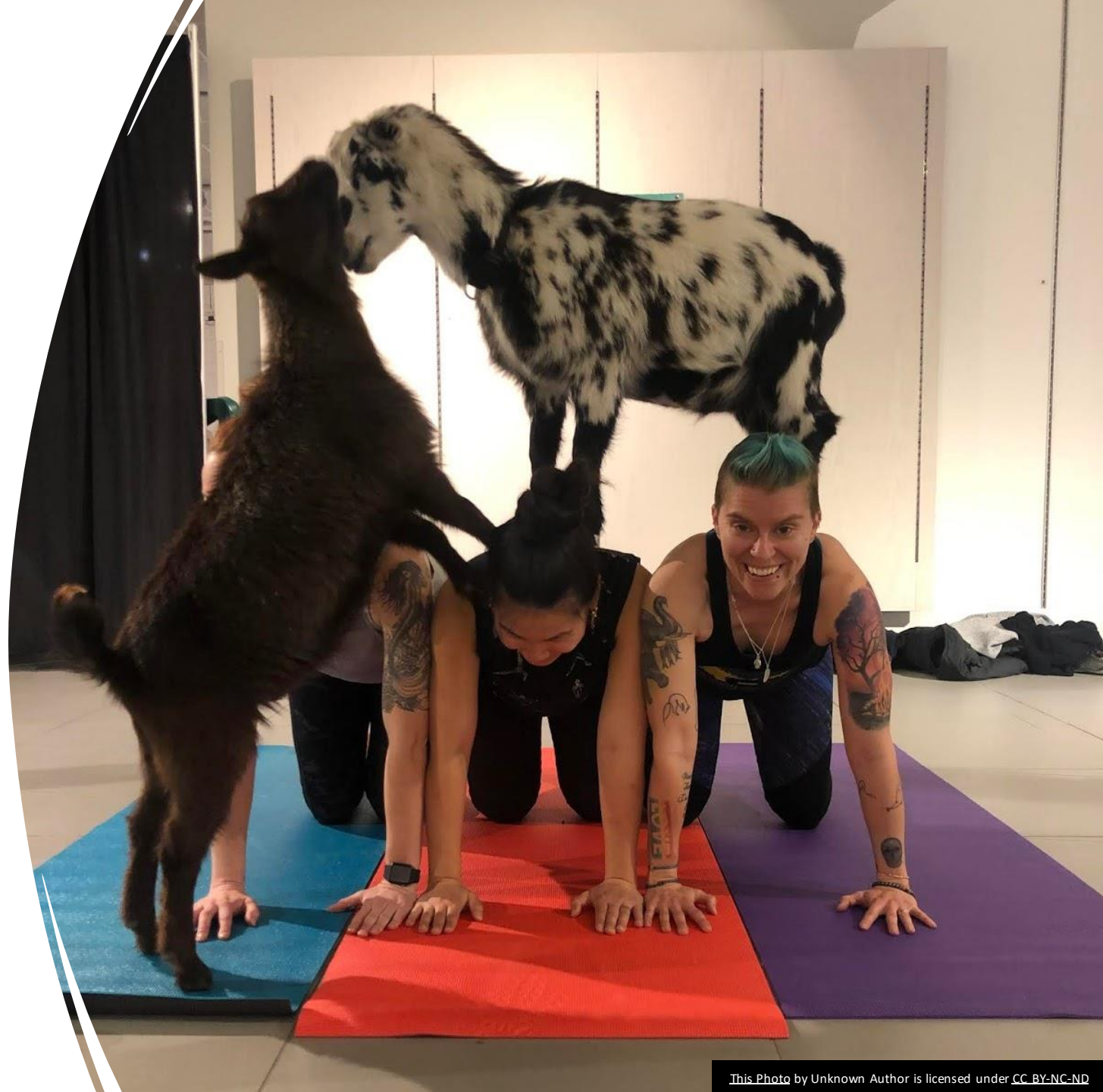
- Mix of letters
- Mix of Numbers
- Special Characters [!\*@#?%^({\$}]
- Minimum 8 characters long
- Pass Phrases

# Pass Phrase Tip

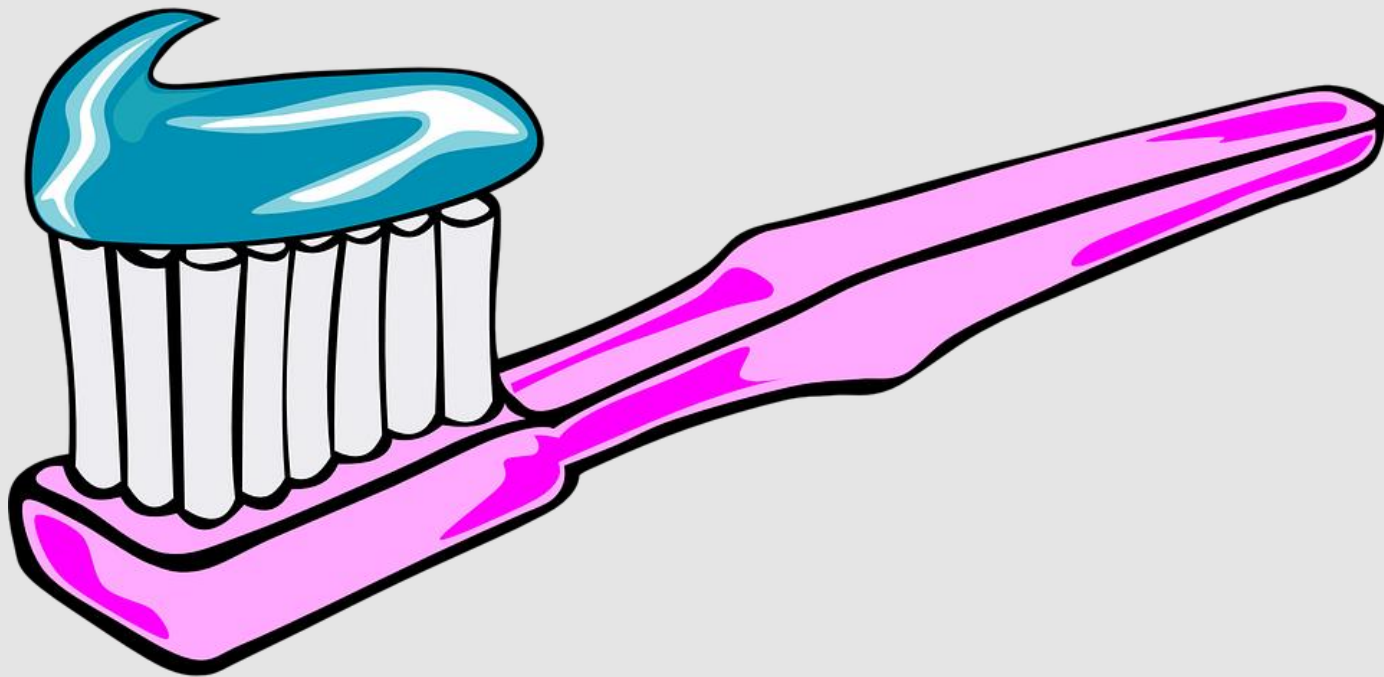
Start with a sentence and replace the letters with numbers, special characters, upper case letters. Using a picture helps you remember the phrase.

2Goats#Ki\$sing@Yoga

The visual will remain in your memory.







Change Your Passwords  
Frequently and Don't share

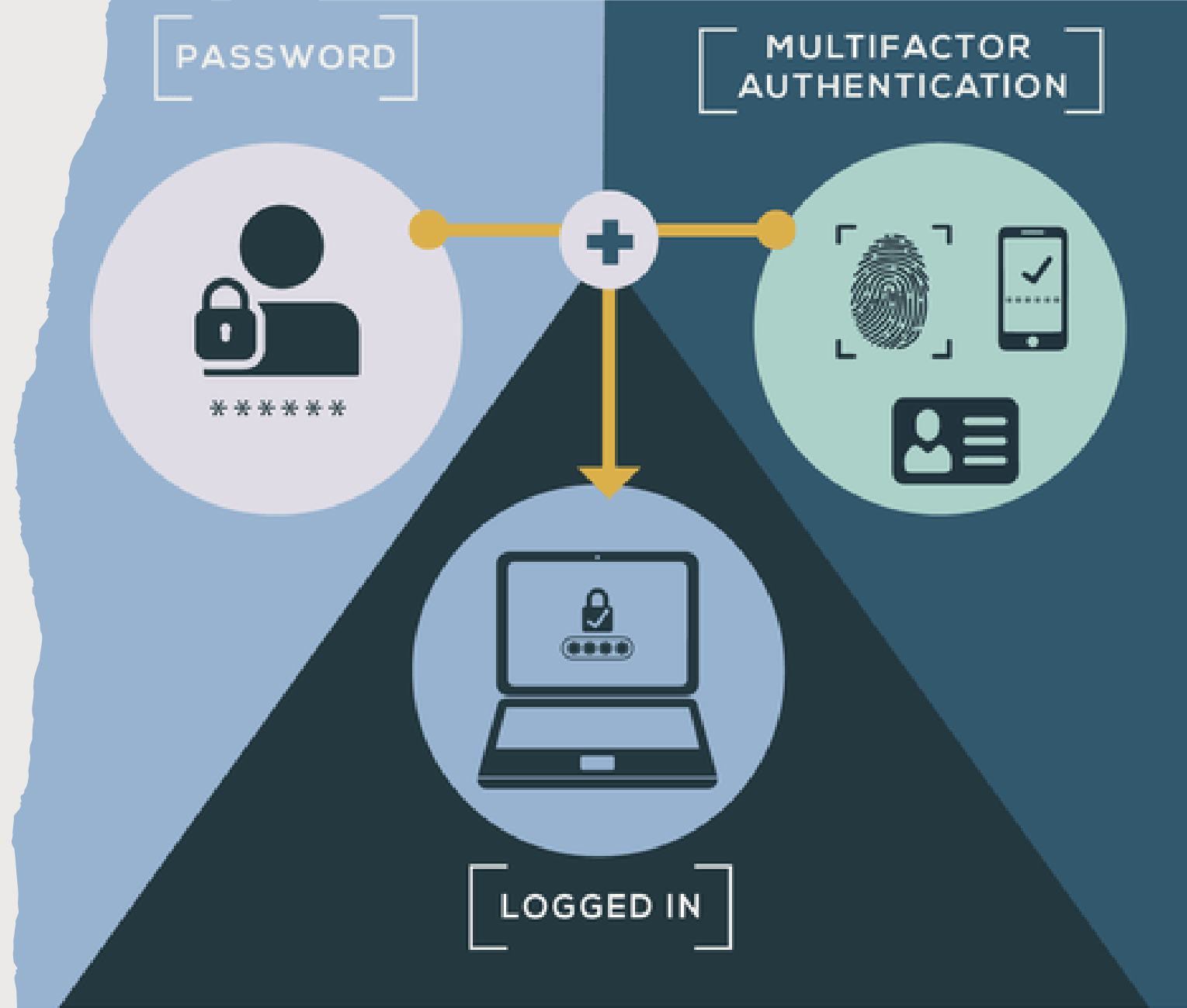
Bet you never thought your password was like a toothbrush.

Well it is.

For your toothbrush to do its job, it needs to be changed regularly. Likewise, for a password to offer good protection, it needs to be changed regularly. Often hackers will break into an account and keep using it. If you change your password, the hacker is no longer able to use your account.

# MFA

- Set up MFA where possible





## PATCHES

- Regular Software updates
- Update your phone software
- Update 3<sup>rd</sup> party software



**Phishing**

# PHISHING

- Emails
- smishing
- Report it

# Phishing

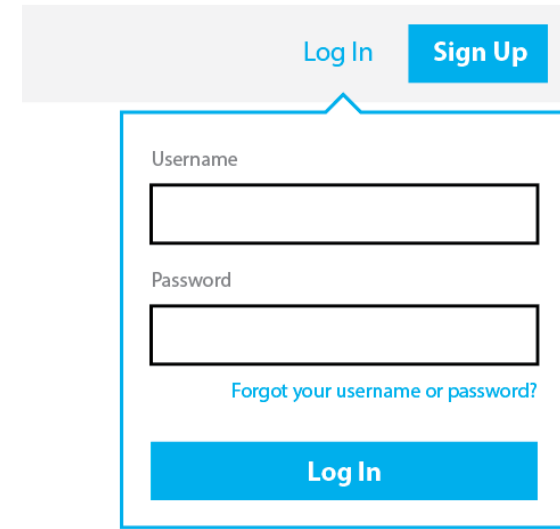
## The Success of Phishing Attacks

Over 255 million phishing attacks in 2022. Another recent study found 3.89% of employees either clicked on a malicious link, forwarded a malicious email or replied to a malicious email.

The impact is disastrous. Just one example is the infiltration of more than 100 banks in 30 countries by cybercriminals, resulting in theft of more than one billion dollars over a two-year period according to Kaspersky lab and it all started with spear phishing attacks.

# Phishing Messages

A phishing message can arrive by email, phone (call, voice mail or text), social networking message, instant message (IM), or fax. The message will ask you to take an action like clicking on a link and entering information on a website, or calling a phone number. Whatever the message, the goal is to get you to reveal private information like your password, account number, or birth date.



Log In Sign Up

Username

Password

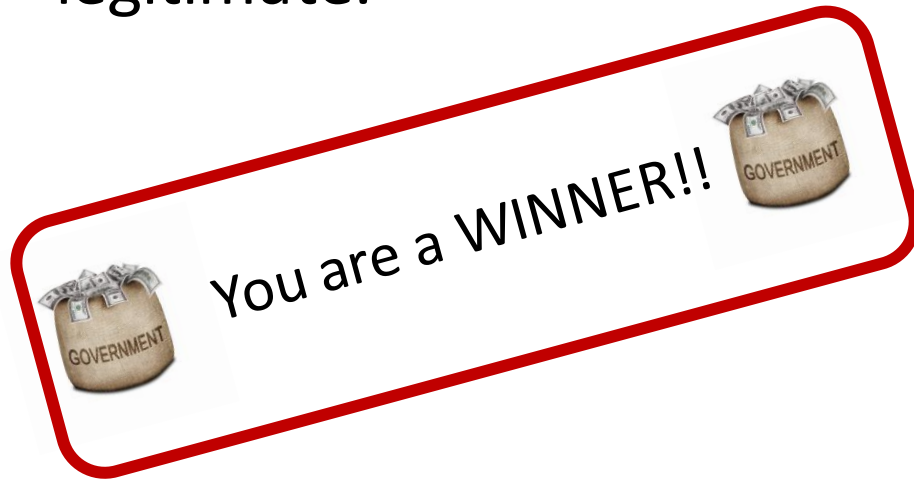
[Forgot your username or password?](#)

Log In



# But why do we fall for it? Why do we take the phishing bait?

Phishers are masters of disguise, making malicious messages look legitimate.



Click here to claim  
your [Amazon](#) \$100 gift  
card.

# But why do we fall for it? Why do we take the phishing bait?

## Curiosity

High profile news stories, gossip, and celebrity photos have some of the highest page views on the Internet. That's why phishers send so many phishing messages related to these topics.

Check out Taylor Swift's new song.



[Click here for World Cup celebration pictures](#)



But why do we fall for it? Why do we take the phishing bait?

## Fear

The phisher warns you that something bad has happened or will happen, and tells you what you should do.

Example phishing message:

Notice of Unpaid Taxes. Review the attached tax statement.

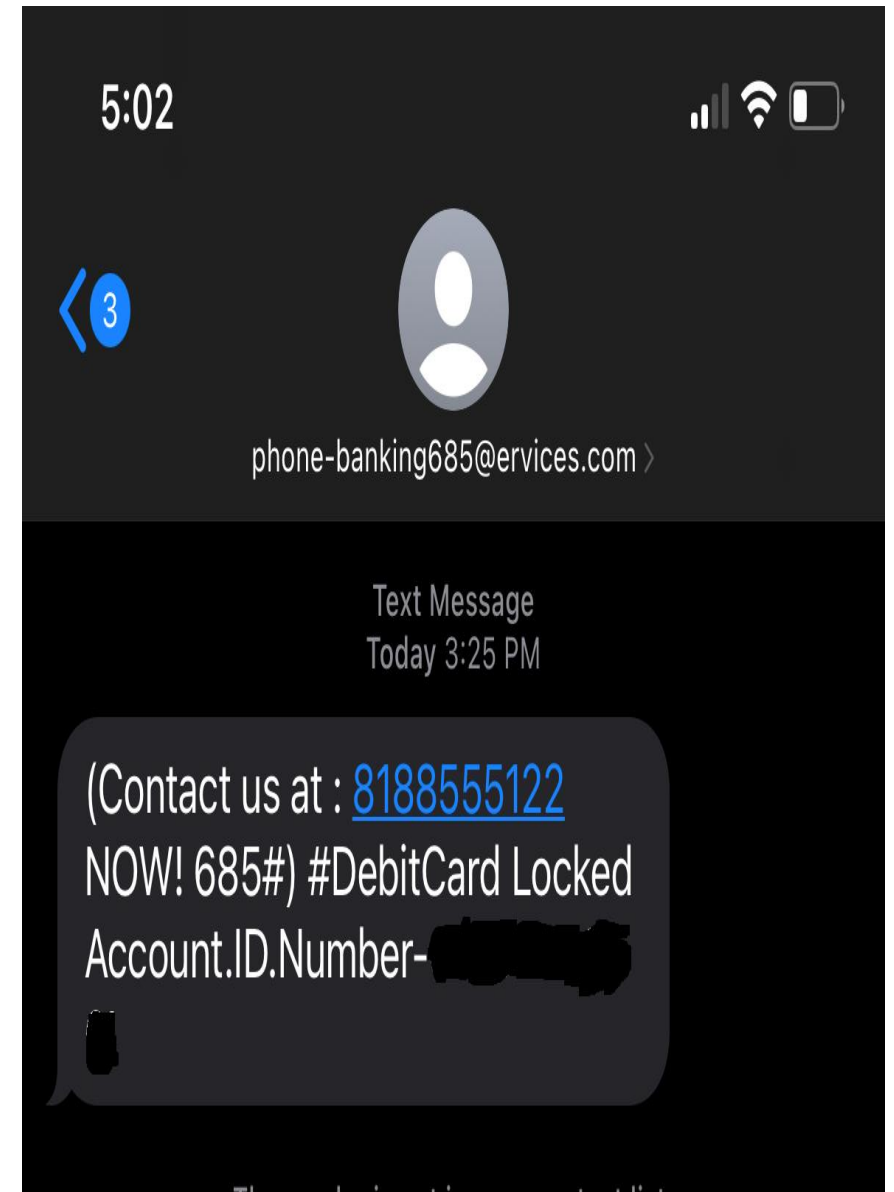


# Phishing Clues

## Trust:

You are out of town, and you just walked out of a store where you just used the card.

What are the clues that this could be a phishing text?



# Help, I think I was Phished!

Despite your best efforts, you think that you were phished. What should you do now?

## At Work:

- Stop what you are doing.
- Call your IT security team or help desk

## At Home:

- If you exposed a password, change it immediately.
- Jot down everything you can remember about what happened.
- Call the account provider and tell them exactly what happened. Refer to your notes.
- If you are the victim of identity theft, have credit bureaus put fraud alerts on your credit reports.
- Close any accounts that were tampered with.
- In the US, report identity theft to the police and Federal Trade Commission (FTC).



# PEOPLE

- Make sure files are backup
- Test backups
- Off-site backup

# Data Backups

Your data is what business is built on: Make backups and avoid the loss of information critical to operations.

Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted. Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.



[This Photo](#) by Unknown Author is licensed under [CCBY-SA-NC](#)

# BACKUPS



Your Systems

Identify where  
you information  
is stored.

# Five's "P" of Cybersecurity

- **PEOPLE**

- **PHISHING**

- **PASSWORD**

- **PEOPLE**

- **PATCHES**



# Questions, Comments or Snide Remarks

Nathan Abbott

[Nathan.Abbott@cot.tn.gov](mailto:Nathan.Abbott@cot.tn.gov)

615-401-7842

[tncot.cc/cyberaware](http://tncot.cc/cyberaware)

TENNESSEE COMPTROLLER OF THE TREASURY

