

# Cybersecurity For Contractors & Engineers



**Central Texas**  
Technology Solutions



# Welcome

## What You Can Do Now to Protect Your Business from Viruses, Malware, Hackers, and Thieves!





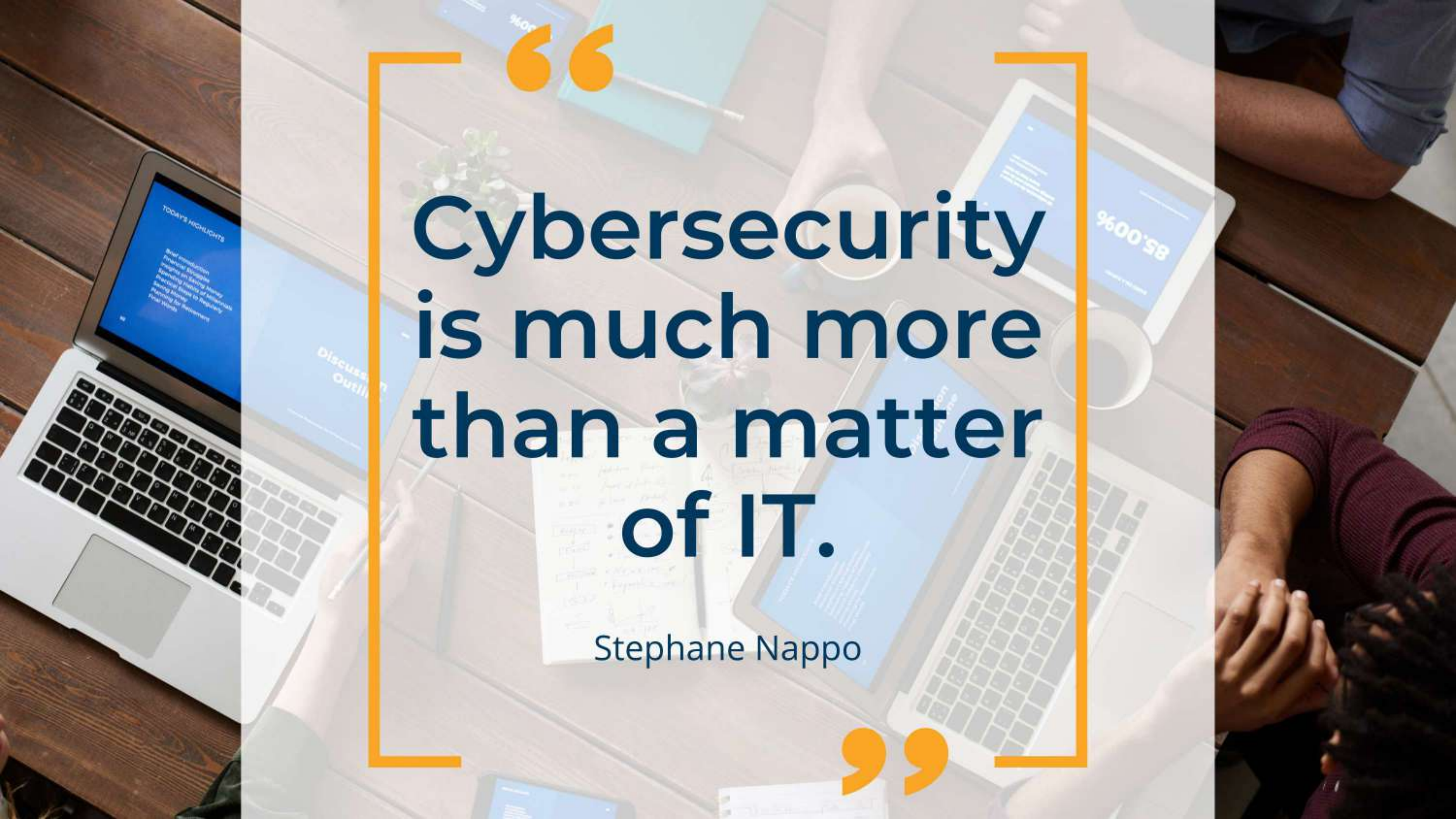


# **When We're Done**

**Free Dark Web Scan for Each Attending Business**

**Download Presentation Slides in PDF format**



A top-down view of a meeting table with laptops, tablets, notebooks, and people's hands. The table is light-colored wood. On the left, a silver laptop is open, displaying a blue screen with white text. Next to it is a tablet showing a blue screen with white text. In the center, there are several notebooks and papers, some with handwritten notes. On the right, another silver laptop is open, displaying a blue screen with white text. A tablet next to it shows a blue screen with white text. People's hands and arms are visible around the table, indicating a collaborative meeting environment. The background is slightly blurred, showing more of the table and the people's hands.

**Cybersecurity  
is much more  
than a matter  
of IT.**

Stephane Nappo





# What You'll Learn:

1. HOW CYBERSECURITY TECHNOLOGY CAN PROTECT YOU AND YOUR BUSINESS
2. THE TACTICS CYBERCRIMINALS USE TO STEAL YOUR DATA
3. BEST PRACTICES TO KEEP YOUR BUSINESS SAFE







**Central Texas**  
Technology Solutions



## About CTTS

For 21 years CTTS has been providing IT Services and Support to Small Businesses and Non-Profits throughout Central Texas.



512-388-5559



[CTTSONline.com](http://CTTSONline.com)



557 S Interstate 35, Suite #201  
Georgetown, TX 78626





# Objective

To Protect your business with cybersecurity awareness and a straightforward cybersecurity strategy.

**Bottom Line - Your business is meaningful - it deserves to be protected.**





# The Challenge

Businesses don't protect their information with the full respect it deserves.

Small businesses with limited resources aren't implementing the security they need, thinking they are too small or insignificant for cyberattacks.

Business leaders are left with either a false sense of security or in a constant state of fear of the looming, imminent threats of a cyber attack.

Your business is important to your family, your employees, your clients, and your communities, and they deserve to be treated and protected as such.





# What's at Stake?

Your entire business could be compromised in the event of a cyber attack.

Personal and financial information of employees and clients could be made public or held for ransom.

The reputation of your business could diminish both within the eyes of your employees and the community.







# Cybersecurity Statistics

---

**46%**

Percentage of global cyberattacks being directed toward Americans.

**58%**

Percentage of cyberattacks from nation-states originated in Russia.

**60%**

Percentage of small companies that go out of business within six months of falling victim to a data breach or cyber attack.





# Most Common Attacks

1. PHISHING / SPOOFING /  
SOCIAL ENGINEERING







# Most Common Attacks

1. PHISHING / SPOOFING /  
SOCIAL ENGINEERING
2. COMPROMISED / STOLEN  
DEVICES







# Most Common Attacks

1. PHISHING / SPOOFING /  
SOCIAL ENGINEERING
2. COMPROMISED / STOLEN  
DEVICES
3. CREDENTIAL THEFT /  
IDENTITY THEFT





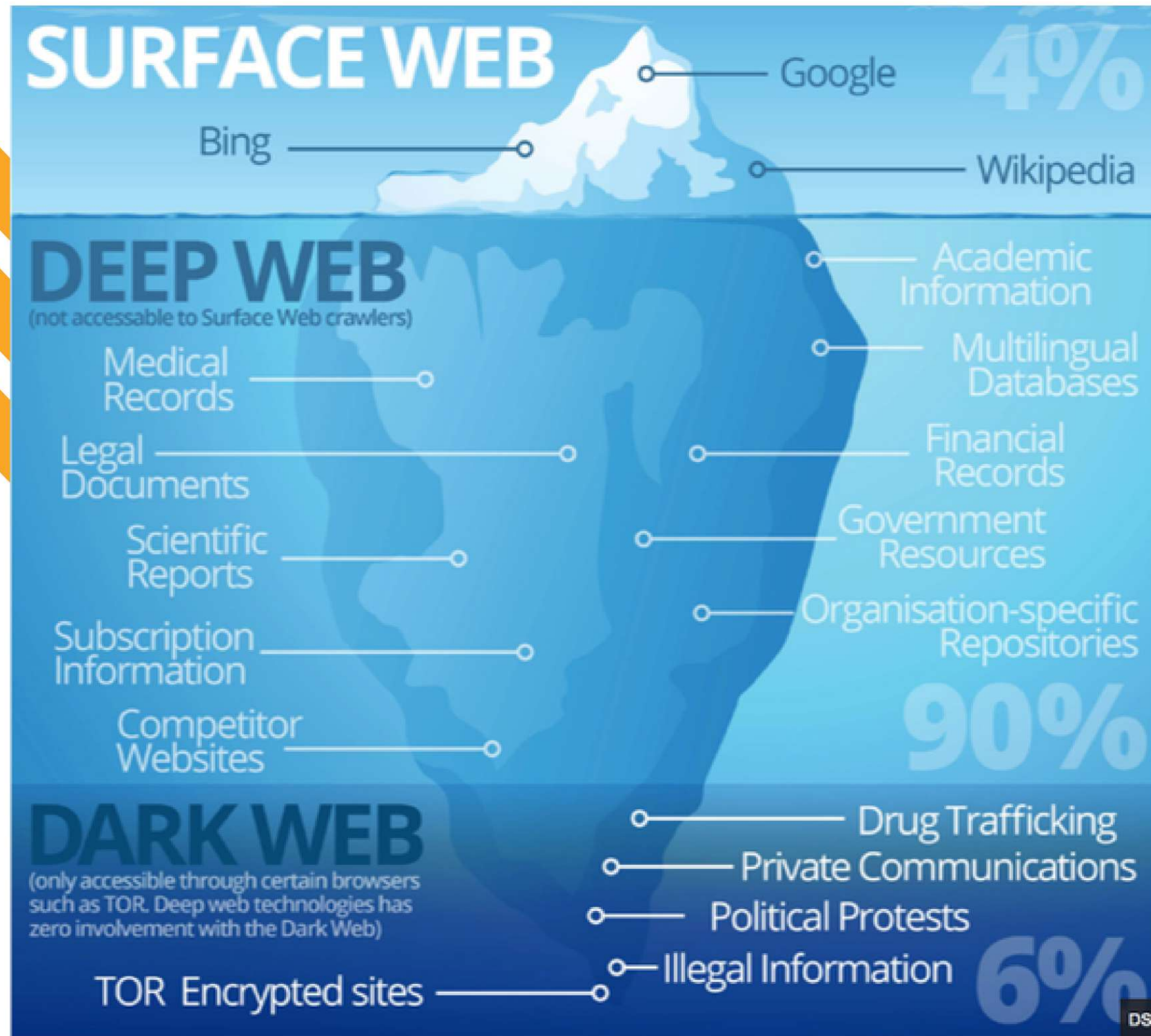
# What is The Dark Web?

---

A hidden universe contained within the “deep web,” a sub layer of the Internet that is hidden from conventional search engines.







# The Dark Web

Search engines like Google and Bing only search 4% of the entire Internet. The other 96% of the web consists of databases, private academic and government networks, and the dark web.

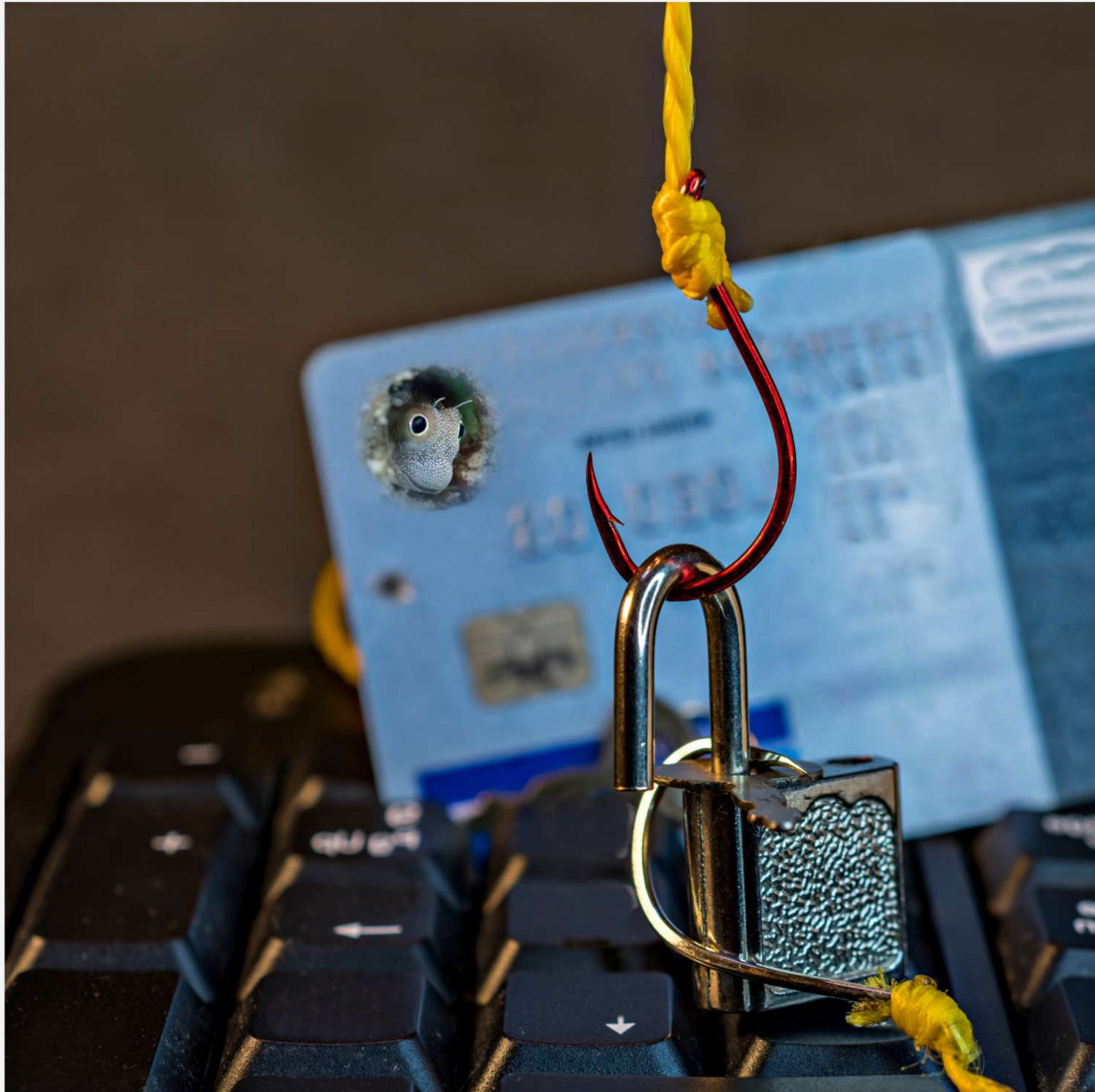


A top-down view of a meeting table. On the left, a silver laptop is open, displaying a blue screen with white text under the heading 'TODAY'S HIGHLIGHTS'. The text includes 'Brief introduction', 'Financial Overview', 'Engage in Saving Money', 'Spending Review of Substantive', 'Security Review of Substantive', 'Reviewing for Retirement', and 'Final Words'. To the right of the laptop, a tablet displays '85.00%' and another tablet displays '%00.58'. There are several blue sticky notes with white text, some of which say 'Discussion Outline'. A white coffee cup is also on the table. In the center, there are some small white flowers. The background shows the legs and arms of people sitting around the table.

**Human error  
accounts for  
95% of all  
cybersecurity  
breaches.**

Source: IBM Cybersecurity Intelligence Index Report





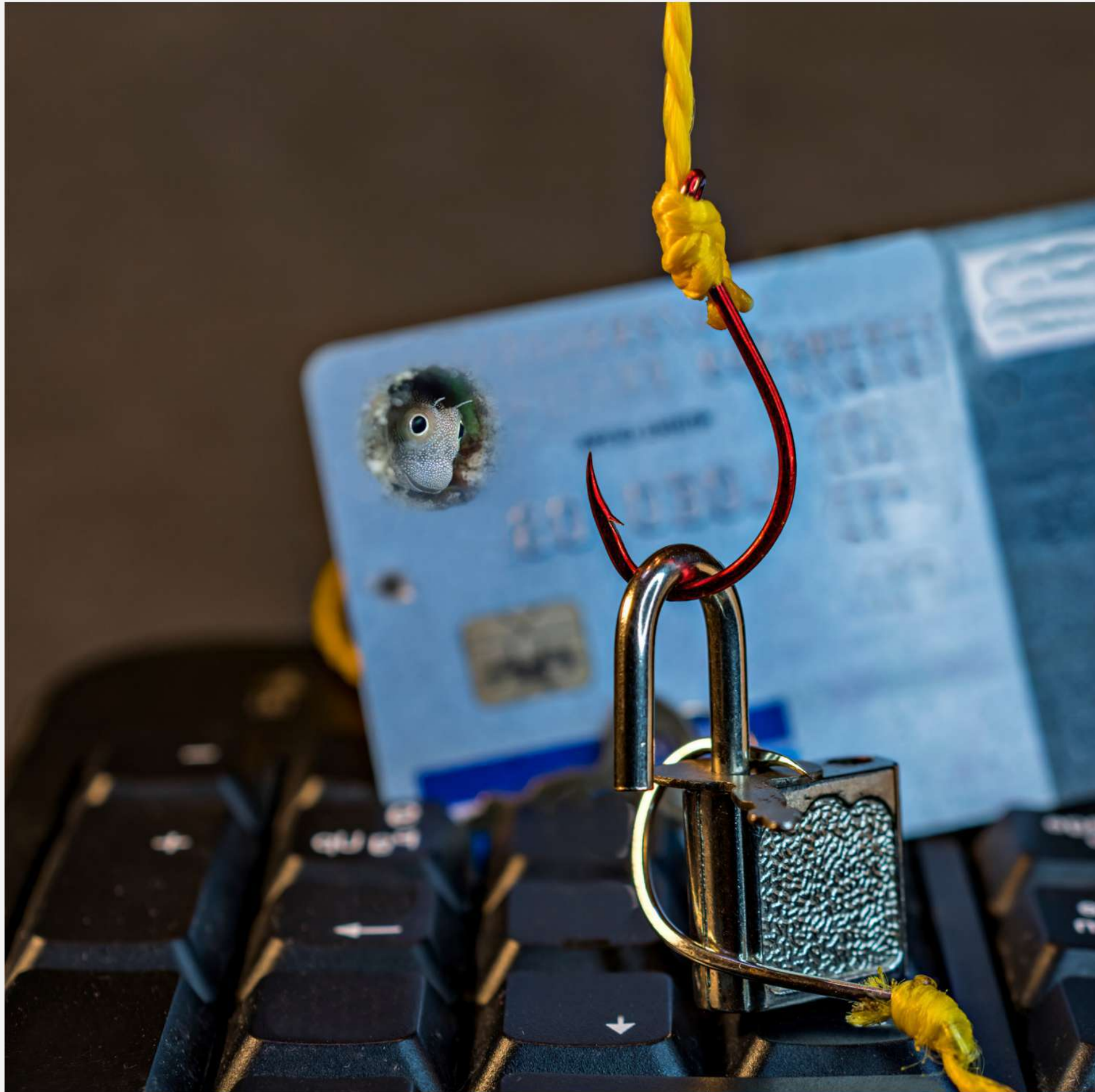
# Cybersecurity at Work

---

## The Biggest Culprits

- Email Compromise
- Social Engineering
- Artificial Intelligence





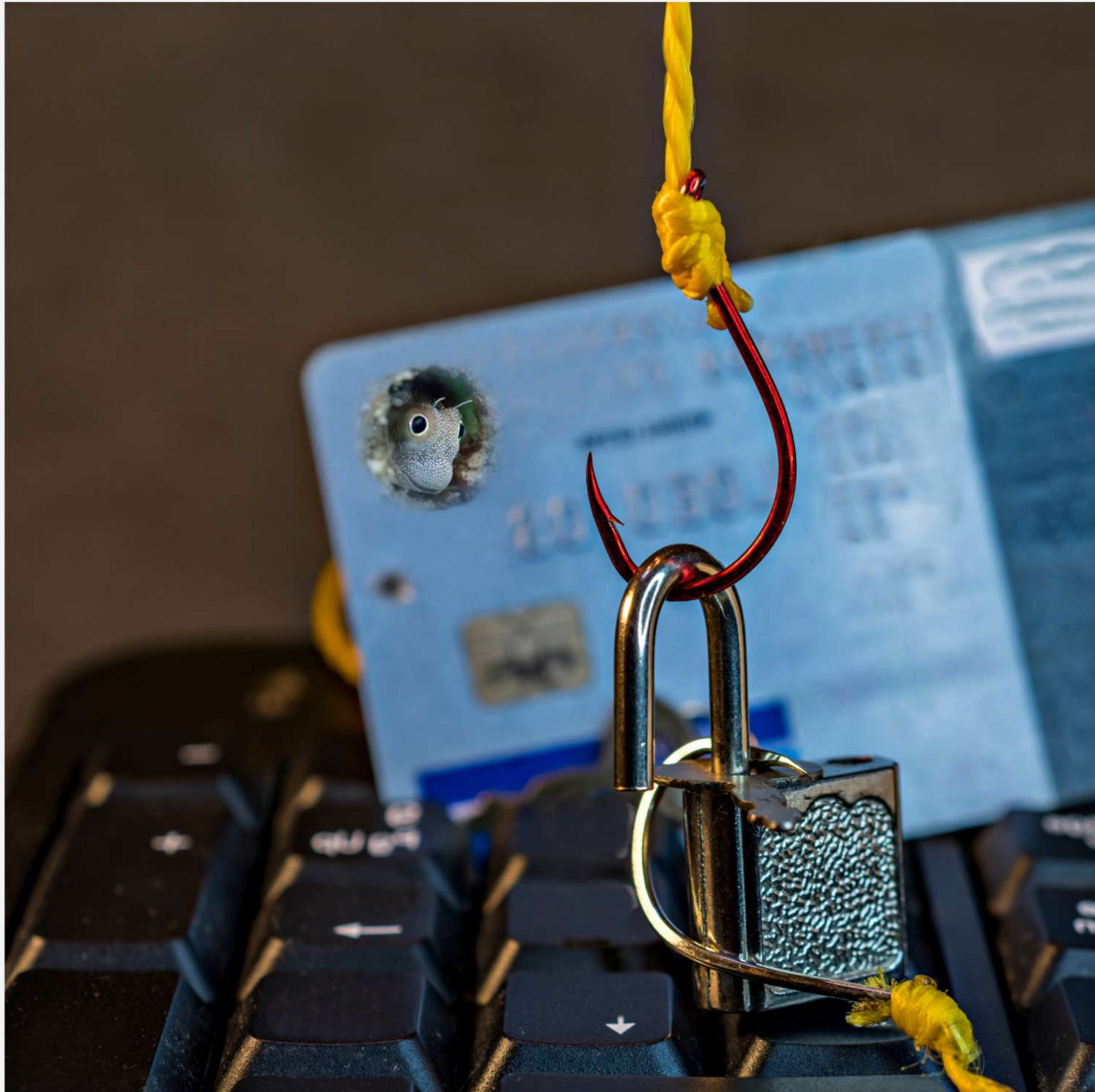
# Cybersecurity at Work

---

## The Goal Behind Them

- Financial Theft
- Data Theft





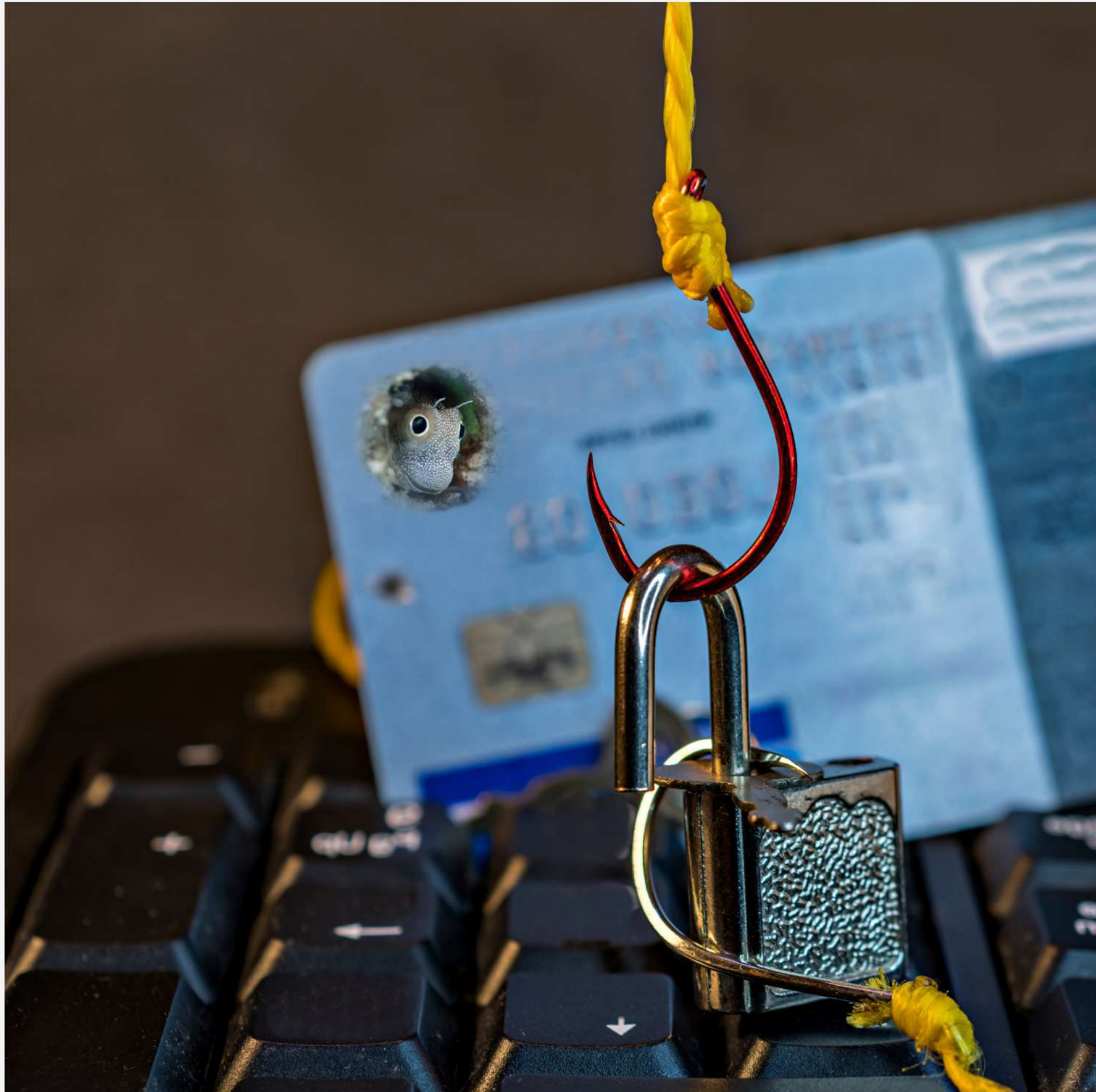
# Cybersecurity at Work

---

## Types of Phishing

- **Spear Phishing** - highly targeted emails to capture logins and cc info
- **Whaling** - targets high-level executives to steal information or send money
- **Smishing** - uses text messages to steal information or send money





# Cybersecurity at Work

---

## Types of Phishing

- **Vishing** - voice phishing to collect sensitive personal information
- **Quishing** - uses a combination of email and QR codes leading to malicious URL
- **Angler Phishing** - social media phishing from fake customer service accounts.





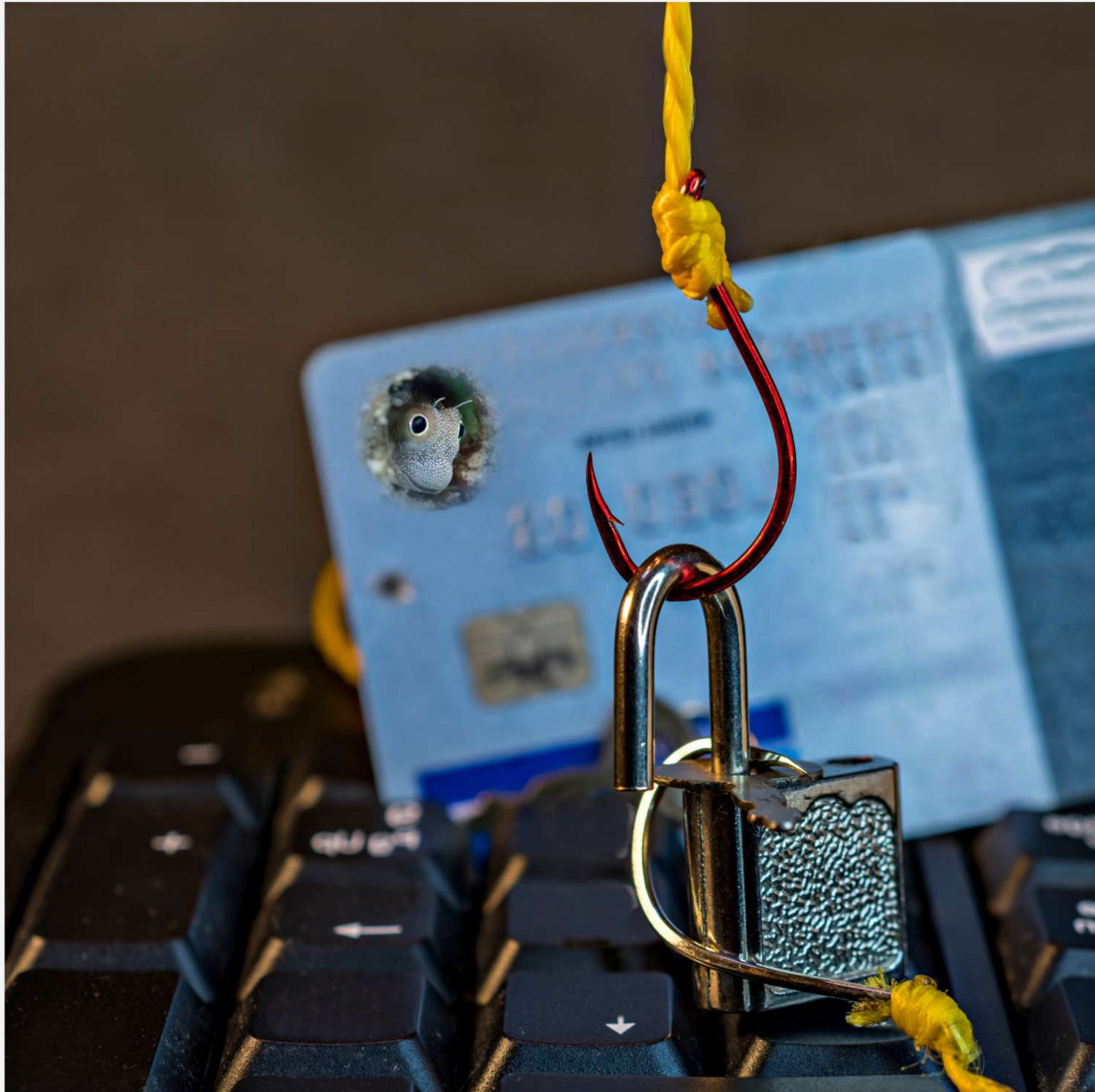
# Cybersecurity at Work

---

## Types of Phishing

- **Business Email Compromise** - spear fishing attack that uses a seemingly legitimate email address to to trick senior-level executives.
- **Brand Impersonation** - emails, texts, voice calls and social media to impersonate a popular business to trick customers into revealing sensitive information.





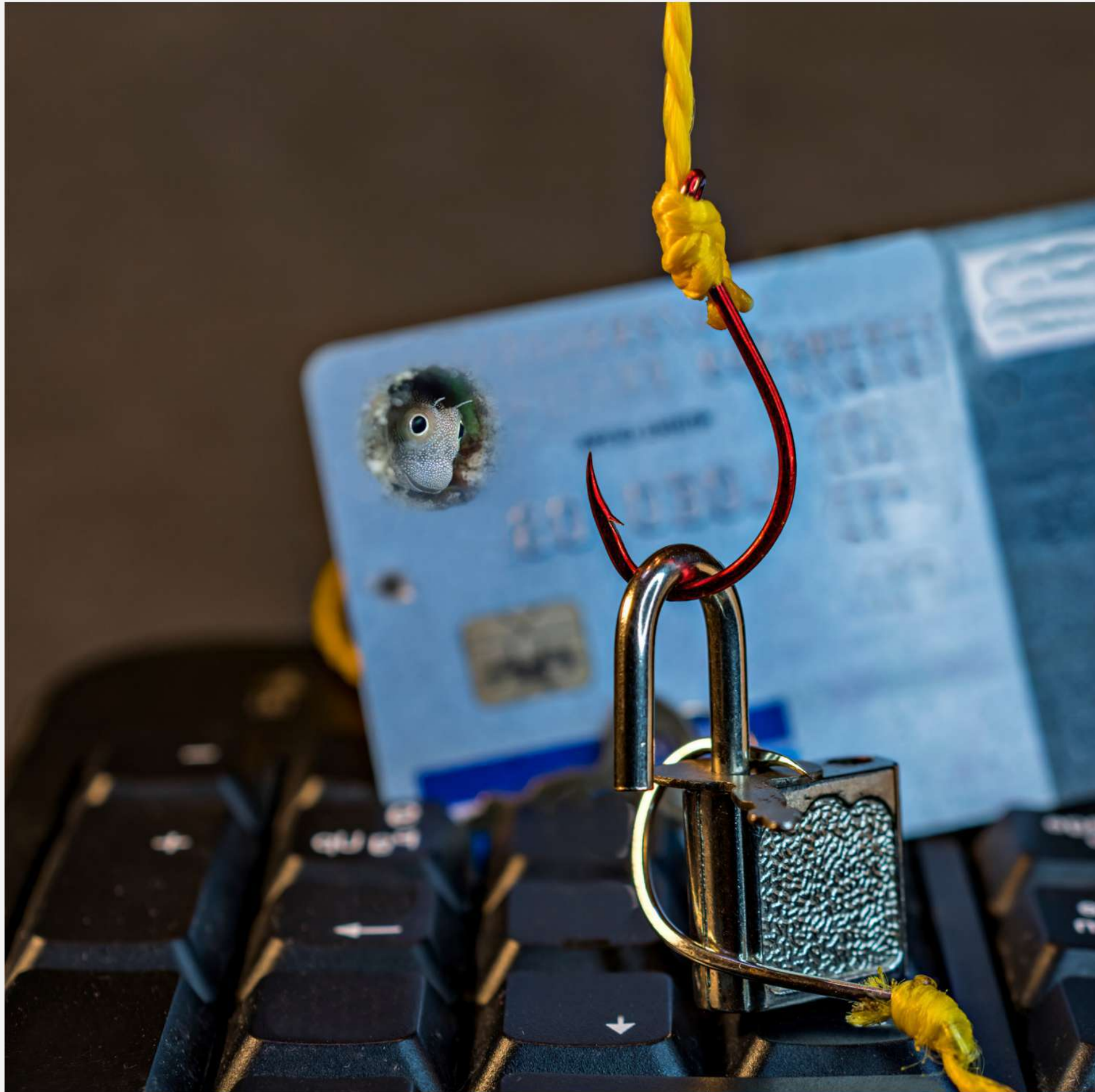
# Cybersecurity at Work

---

**Don't take the bait!**

- In an email ask you to click on a link, be wary. Links can contain malicious software that can steal your data in personal information.
- If an email directs you to a website, be cautious. It could be a malicious site that can steal your personal information such as login credentials.





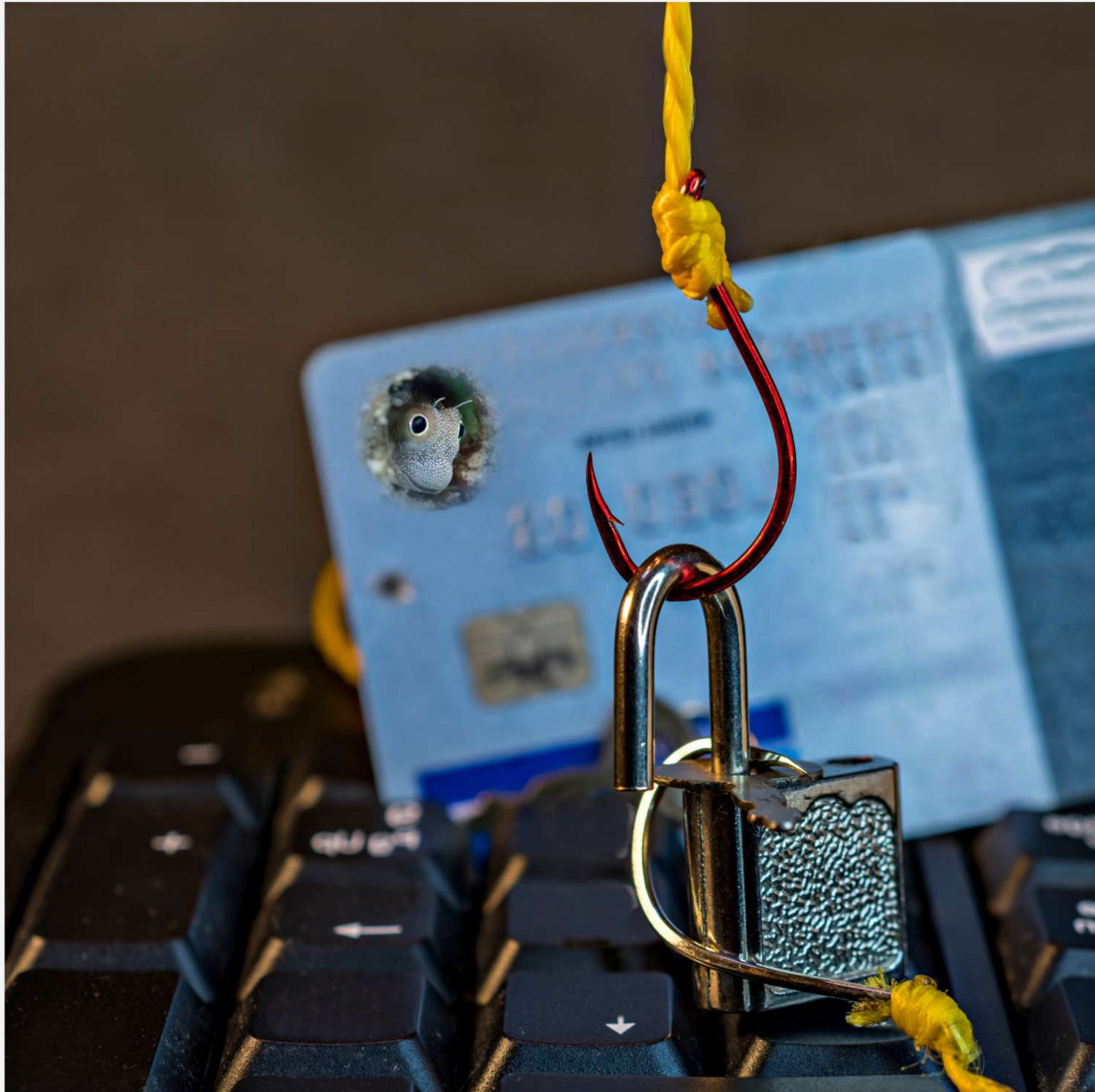
# Cybersecurity at Work

---

**Don't take the bait!**

- If an email contains an attachment, be alert. Malicious extensions disguised to look like a document, invoice or voicemail can infect your computer and steal your info.
- If an email tries to rush you into taking an urgent action, such as transferring funds, be suspicious. Verify the authenticity of the request before taking action.





# Cybersecurity at Work

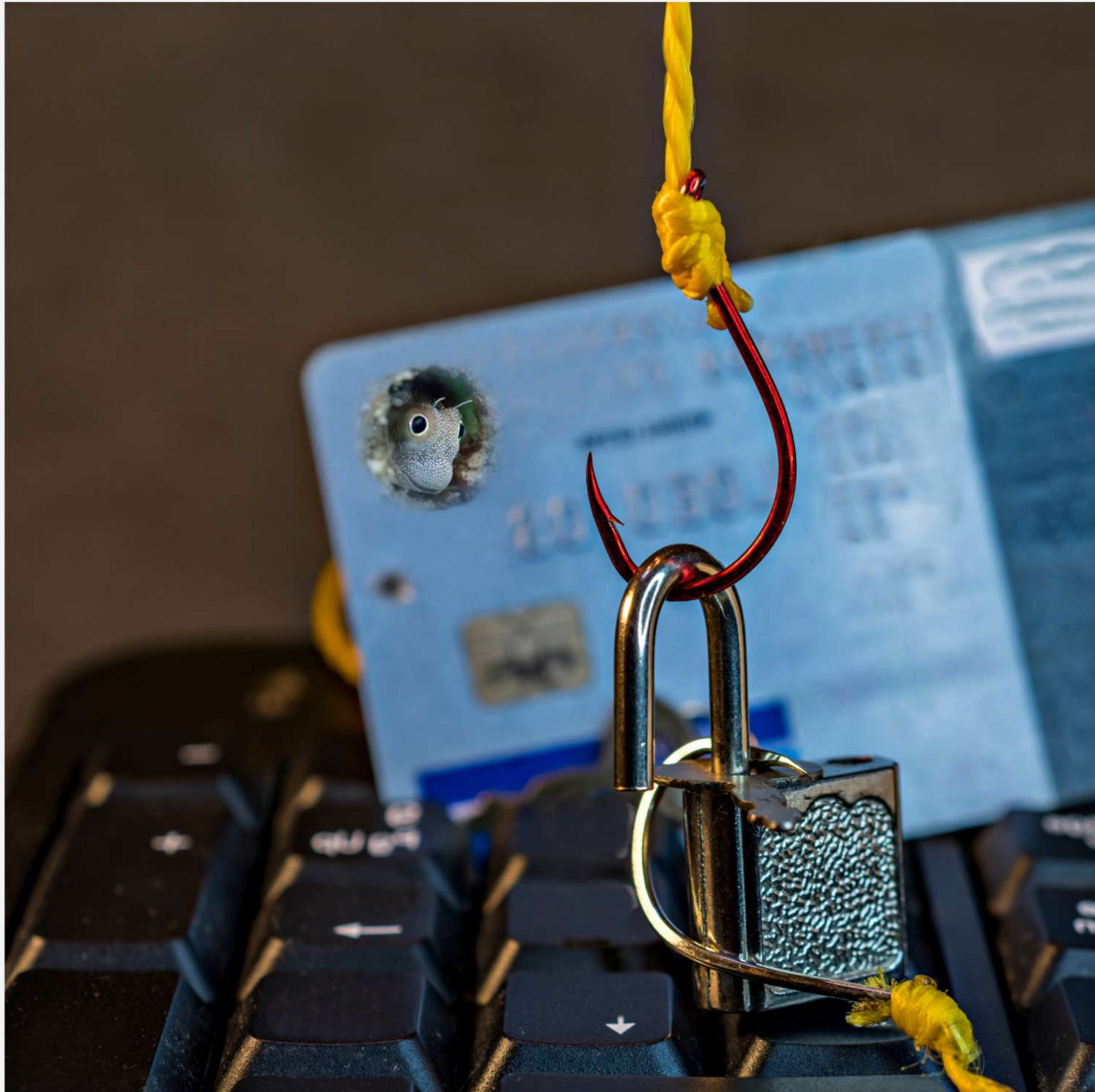
---

**What about AI?**

**The Top Benefits:**

- **Smart Data Analysis**
- **Improved Productivity**
- **Faster Business Maneuvering**





# Cybersecurity at Work

---

**What about AI?**

**The Potential Risks:**

- **AI-Powered Phishing Scams**
- **Malicious AI-Generated Code**
- **Deep Fakes and Impersonations**





# Protect Yourself and Your Organization

---

- Keep your software and anti-virus up-to-date.
- Establish computer usage guidelines for all employees.
- Double-check all email attachments before opening them.







# Protect Yourself and Your Organization

---

- Treat business information as personal information.
- Stay vigilant on Social Media.
- Trust Your Instincts.
- It only takes one time...







# Your Credentials Have Been Compromised - Now What?

1. Alert All Employees







# Your Credentials Have Been Compromised - Now What?

1. Alert All Employees
2. Review Individual Compromises







# Your Credentials Have Been Compromised - Now What?

1. Alert All Employees
2. Review Individual Compromises
3. Establish Strict Password Policies





# TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

## Password Security

Utilizing a password generator or password manager can help you select longer, more complicated passwords that will be extremely difficult to breach.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years



## Time It Takes Using AI to Crack Your Password [2023]



# OF CHARACTER	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	613M Years	14Bn Years
16	2 Days	23K Years	2Bn Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.23Bn Years	96Tn Years	6Qn Years

# Password Security

Utilizing a password generator or password manager can help you select longer, more complicated passwords that will be extremely difficult to breach.





# Your Credentials Have Been Compromised - Now What?

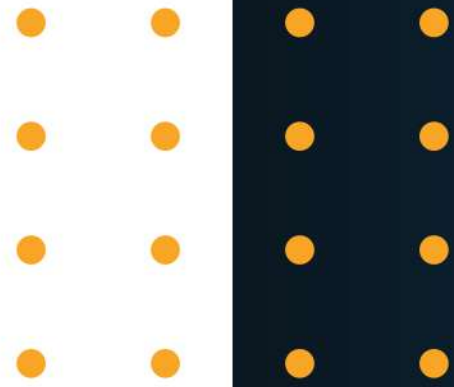
1. Alert All Employees
2. Review Individual Compromises
3. Establish Strict Password Policies
4. Change Passwords for All Exposed Logins





# Best Practices

---



01

Implement Multi-Factor Authentication, or MFA

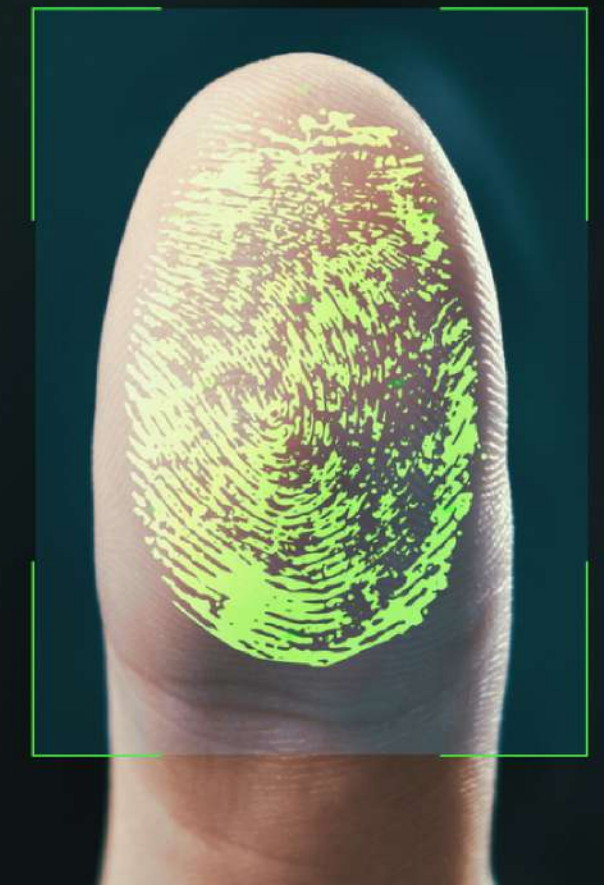
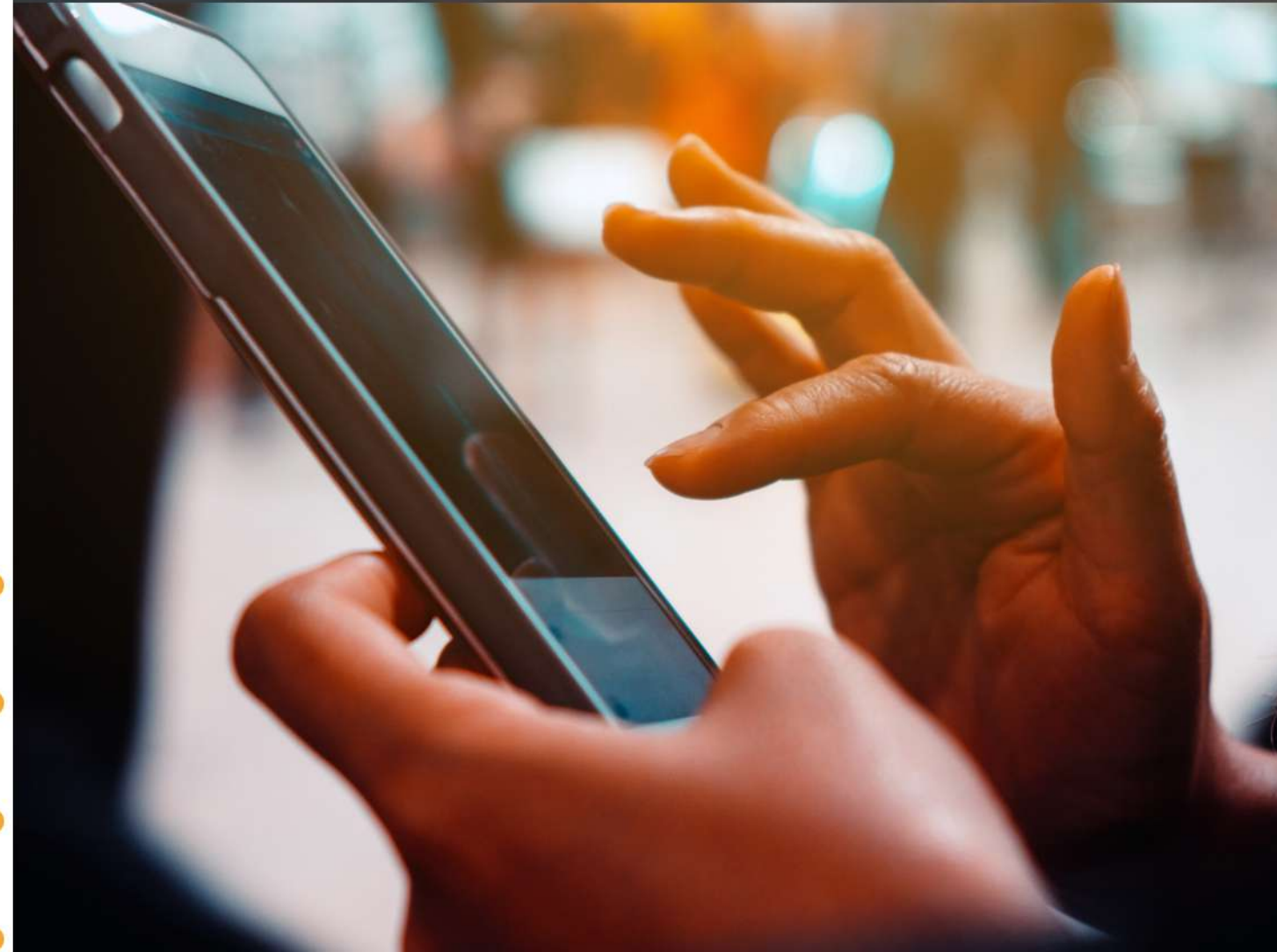




# MFA / 2FA

---

A security process that requires more than one method of authentication from independent sources to verify your identity.





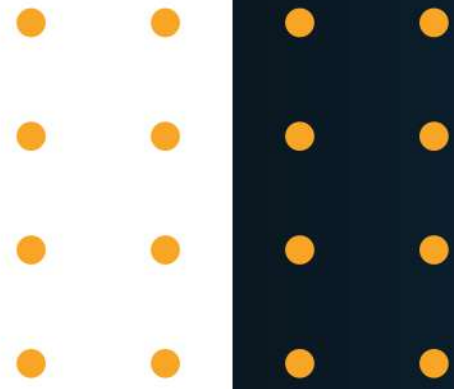
A top-down view of a collaborative workspace. Several laptops and tablets are open on a light-colored wooden table. People's hands and arms are visible, interacting with the devices. One laptop screen shows 'TODAY'S HIGHLIGHTS' with a list of items. Another tablet displays '85.00%' and '85.00%'. A tablet in the center shows 'Discussion Outline'. A small potted plant is on the table. The background is a dark wooden wall.

**MFA stops  
99% of  
password-  
based cyber  
crimes.**



# Best Practices

---



02

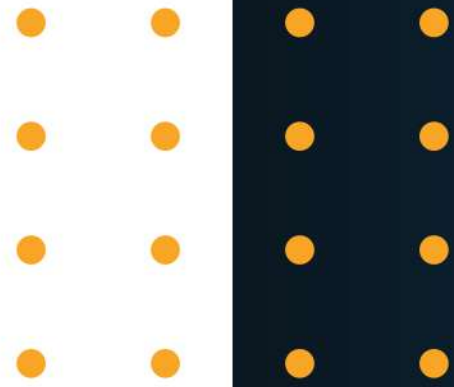
Provide Ongoing Security  
Awareness Training





# Best Practices

---



03

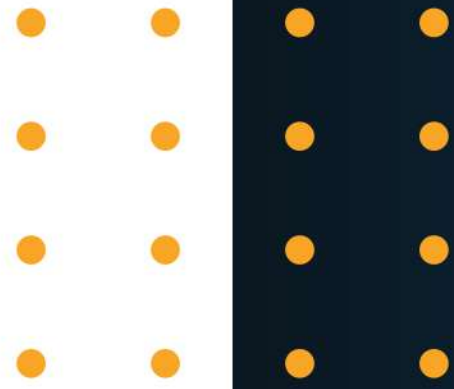
Perform Regular Risk Assessments





# Best Practices

---



04

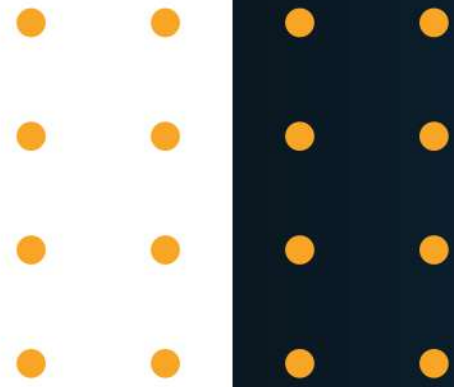
Proactively Monitor for  
Breaches and Cyber Threats





# Best Practices

---



05

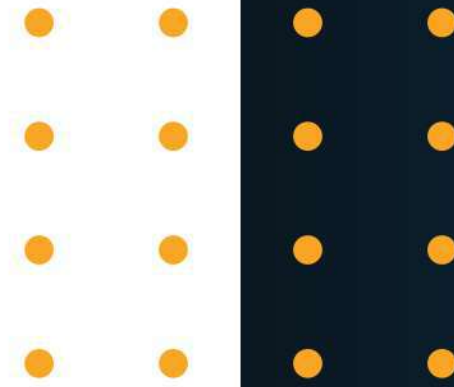
Back Up Everything!





# Best Practices

---



06

Invest in Cyber Insurance





# 3 Types of Cyber Insurance

---

## Cyber Theft

**First-Party Coverage**

**Embezzlement**

**Scams - phony invoices,  
money transfers, etc.**





# 3 Types of Cyber Insurance

---

## Cyber Liability

**Third-Party Coverage**

**Regulatory Penalties**

**Lawsuits**





# 3 Types of Cyber Insurance

---

## Cyber Extortion

**Ransom**

**Negotiations**

**Forensics**







**Questions?**



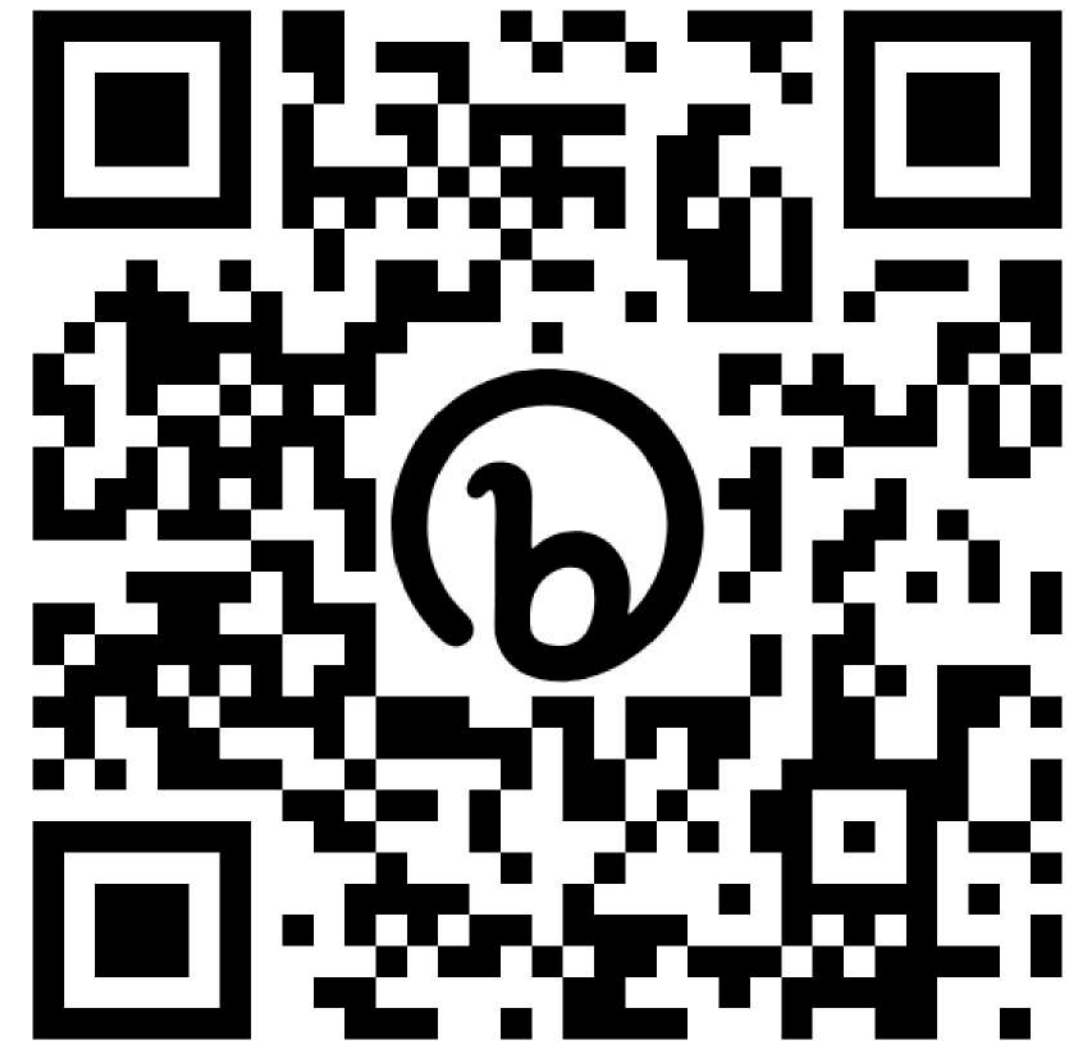


# Next Steps

**Free Dark Web Scan for Each Business**

**Download Presentation Slides**

<https://cttsonline.com/acealunch>





# Contact Us

---



512-388-5559



CTTSONline.com



557 S Interstate 35, Suite #201  
Georgetown, TX 78626





# THANK YOU!



**Central Texas**  
Technology Solutions