DOUGLAS COUNTY CYBERSECURITY AWARENESS MONTH eBook

From the Douglas County CTO and the Information Services Department's Division of Cybersecurity

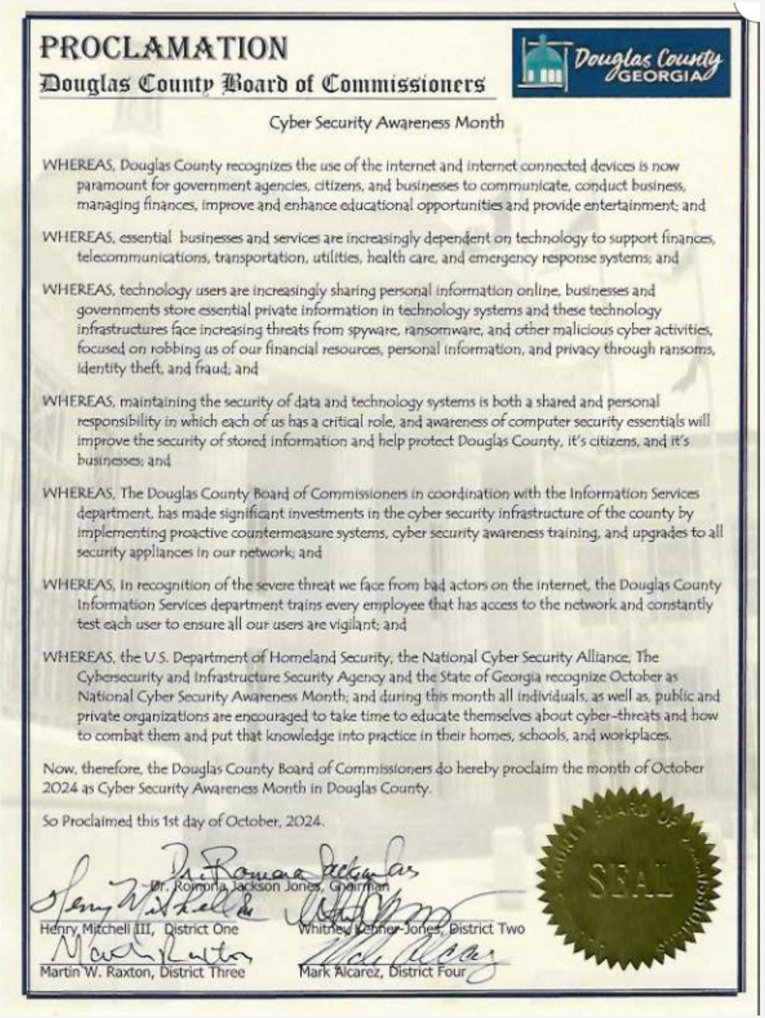
DOUGLAS COUNTY
GEORGIA

A message From the Douglas County CTO and the Information Services Department's Division of Cybersecurity.

Welcome to the Cybersecurity Awareness Month 2024 eBook, hosted by the Douglas County CTO and the Information Services Department's Division of Cybersecurity. The month of October is now designated as Cybersecurity Awareness Month in our community, aimed at educating and empowering both citizens and employees to safely navigate the digital world.

With the rise of cyber threats such as phishing, identity theft, ransomware, and more, it's critical that we all stay vigilant and informed. This eBook will provide essential knowledge and best practices to help you stay protected against these ever-growing online dangers.

DOUGLAS COUNTY
GEORGIA



PROCLAMATION

Douglas County Board of Commissioners

Douglas County GEORGIA

Cyber Security Awareness Month

WHEREAS, Douglas County recognizes the use of the internet and internet connected devices is now paramount for government agencies, citizens, and businesses to communicate, conduct business, managing finances, improve and enhance educational opportunities and provide entertainment; and

WHEREAS, essential businesses and services are increasingly dependent on technology to support finances, telecommunications, transportation, utilities, health care, and emergency response systems; and

WHEREAS, technology users are increasingly sharing personal information online, businesses and governments store essential private information in technology systems and these technology infrastructures face increasing threats from spyware, ransomware, and other malicious cyber activities, focused on robbing us of our financial resources, personal information, and privacy through ransoms, identity theft, and fraud; and

WHEREAS, maintaining the security of data and technology systems is both a shared and personal responsibility in which each of us has a critical role, and awareness of computer security essentials will improve the security of stored information and help protect Douglas County, it's citizens, and it's businesses; and

WHEREAS, The Douglas County Board of Commissioners in coordination with the Information Services department, has made significant investments in the cyber security infrastructure of the county by implementing proactive countermeasure systems, cyber security awareness training, and upgrades to all security appliances in our network; and

WHEREAS, In recognition of the severe threat we face from bad actors on the internet, the Douglas County Information Services department trains every employee that has access to the network and constantly test each user to ensure all our users are vigilant; and

WHEREAS, the U.S. Department of Homeland Security, the National Cyber Security Alliance, The Cybersecurity and Infrastructure Security Agency and the State of Georgia recognize October as National Cyber Security Awareness Month; and during this month all individuals, as well as, public and private organizations are encouraged to take time to educate themselves about cyber-threats and how to combat them and put that knowledge into practice in their homes, schools, and workplaces.

Now, therefore, the Douglas County Board of Commissioners do hereby proclaim the month of October 2024 as Cyber Security Awareness Month in Douglas County.

So Proclaimed this 1st day of October, 2024.

Dr. Romona Jackson Jones
Dr. Romona Jackson Jones, Chairman

Henry Mitchell
Henry Mitchell III, District One

Whitney Kebner-Jones, District Two

Martin Raxton
Martin W. Raxton, District Three

Mark Alcarez, District Four

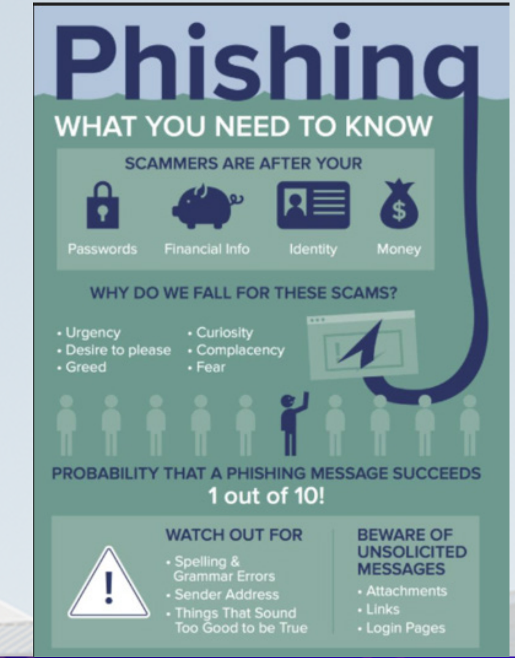
SEAL

Chapter 1

Why Cybersecurity Matters to You?

In today's connected world, we rely heavily on the internet for communication, shopping, and even accessing government services. While this has brought convenience, it has also introduced new threats. Cybercriminals prey on unsuspecting users, and their methods are becoming more sophisticated every year. Whether you're a government employee or a citizen of Douglas County, knowing how to protect yourself online is vital.

DOUGLAS COUNTY
GEORGIA



Phishing

WHAT YOU NEED TO KNOW

SCAMMERS ARE AFTER YOUR

- Passwords
- Financial Info
- Identity
- Money

WHY DO WE FALL FOR THESE SCAMS?

- Urgency
- Desire to please
- Greed
- Curiosity
- Complacency
- Fear

PROBABILITY THAT A PHISHING MESSAGE SUCCEEDS

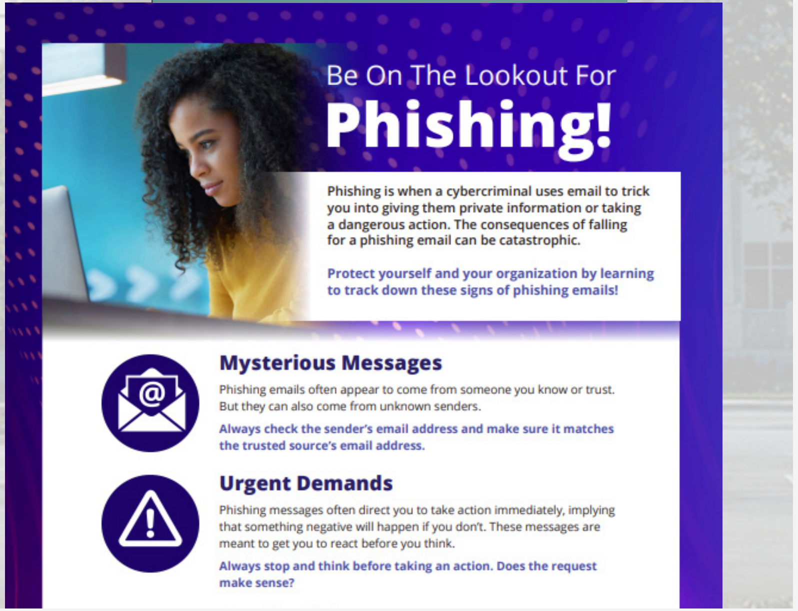
1 out of 10!

WATCH OUT FOR

- Spelling & Grammar Errors
- Sender Address
- Things That Sound Too Good to be True

BEWARE OF UNSOLICITED MESSAGES

- Attachments
- Links
- Login Pages



Be On The Lookout For

Phishing!

Phishing is when a cybercriminal uses email to trick you into giving them private information or taking a dangerous action. The consequences of falling for a phishing email can be catastrophic.

Protect yourself and your organization by learning to track down these signs of phishing emails!

Mysterious Messages

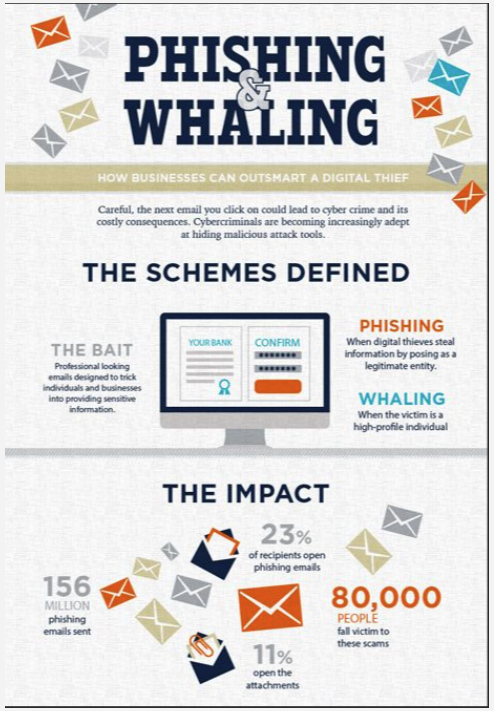
Phishing emails often appear to come from someone you know or trust. But they can also come from unknown senders.

Always check the sender's email address and make sure it matches the trusted source's email address.

Urgent Demands

Phishing messages often direct you to take action immediately, implying that something negative will happen if you don't. These messages are meant to get you to react before you think.

Always stop and think before taking an action. Does the request make sense?



PHISHING & WHALING

HOW BUSINESSES CAN OUTSMART A DIGITAL THIEF

Careful, the next email you click on could lead to cyber crime and its costly consequences. Cybercriminals are becoming increasingly adept at hiding malicious attack tools.

THE SCHEMES DEFINED

THE BAIT
Professional looking emails designed to trick individuals and businesses into providing sensitive information.

PHISHING
When digital thieves steal information by posing as a legitimate entity.

WHALING
When the victim is a high-profile individual

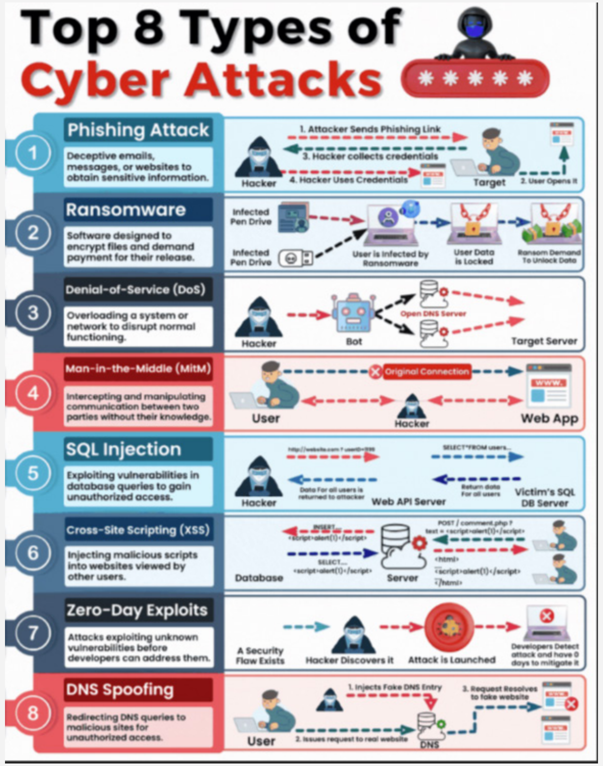
THE IMPACT

156 MILLION phishing emails sent

23% of recipients open phishing emails

11% open the attachments

80,000 PEOPLE fall victim to these scams



Top 8 Types of Cyber Attacks

1 Phishing Attack
Deceptive emails, messages, or websites to obtain sensitive information.

1. Attacker Sends Phishing Link
2. User Opens it
3. Hacker collects credentials
4. Hacker Uses Credentials
Hacker
Target

2 Ransomware
Software designed to encrypt files and demand payment for their release.

Infected Pen Drive
Infected Pen Drive
User is Infected by Ransomware
User Data is Locked
Ransom Demand To Unlock Data

3 Denial-of-Service (DoS)
Overloading a system or network to disrupt normal functioning.

Hacker
Bot
Open DNS Server
Target Server

4 Man-in-the-Middle (MitM)
Intercepting and manipulating communication between two parties without their knowledge.

5 SQL Injection
Exploiting vulnerabilities in database queries to gain unauthorized access.

http://website.com?userID=1199
SELECT*FROM users...
Data for all users is returned to attacker
Return data for all users
Hacker
Web API Server
Victim's SQL DB Server

6 Cross-Site Scripting (XSS)
Injecting malicious scripts into websites viewed by other users.

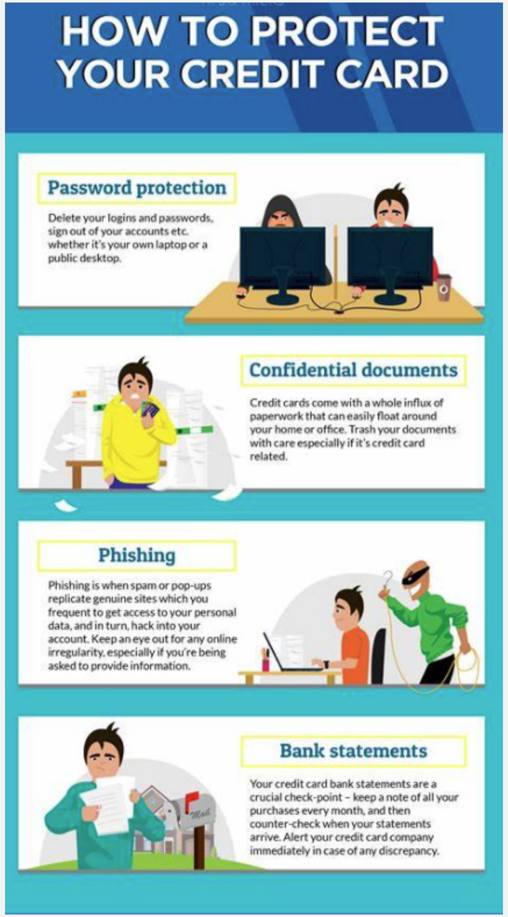
INSERT...
<script>alert(1)</script>
SELECT...
<script>alert(1)</script>
POST / comment.php ?
text = <script>alert(1)</script>
<html>
<script>alert(1)</script>
</html>
Database
Server

7 Zero-Day Exploits
Attacks exploiting unknown vulnerabilities before developers can address them.

8 DNS Spoofing
Redirecting DNS queries to malicious sites for unauthorized access.

1. Injects Fake DNS Entry
2. Issues request to real website
3. Request Resolves to fake website
User
DNS

The Best cybersecurity insight of 2024



HOW TO PROTECT YOUR CREDIT CARD

Password protection

Delete your logins and passwords, sign out of your accounts etc. whether it's your own laptop or a public desktop.

Confidential documents

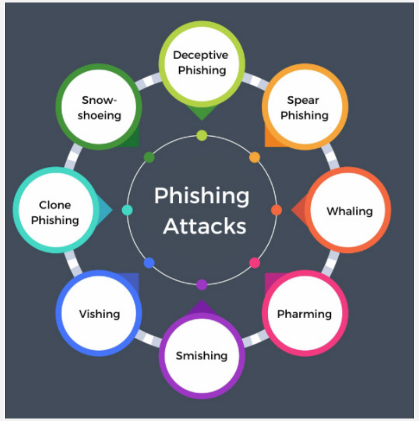
Credit cards come with a whole influx of paperwork that can easily float around your home or office. Trash your documents with care especially if it's credit card related.

Phishing

Phishing is when spam or pop-ups replicate genuine sites which you frequent to get access to your personal data, and in turn, hack into your account. Keep an eye out for any online irregularity, especially if you're being asked to provide information.

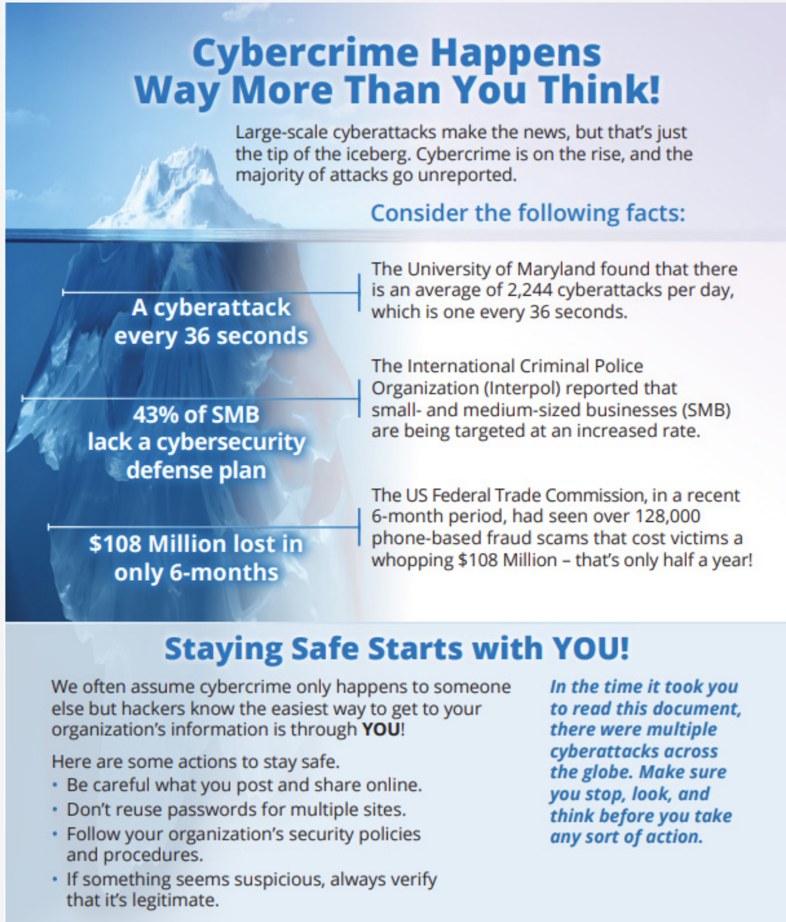
Bank statements

Your credit card bank statements are a crucial check-point – keep a note of all your purchases every month, and then counter-check when your statements arrive. Alert your credit card company immediately in case of any discrepancy.



PHISHING

DOUGLAS COUNTY
GEORGIA



Cybercrime Happens Way More Than You Think!

Large-scale cyberattacks make the news, but that's just the tip of the iceberg. Cybercrime is on the rise, and the majority of attacks go unreported.

Consider the following facts:

A cyberattack every 36 seconds

The University of Maryland found that there is an average of 2,244 cyberattacks per day, which is one every 36 seconds.

43% of SMB lack a cybersecurity defense plan

The International Criminal Police Organization (Interpol) reported that small- and medium-sized businesses (SMB) are being targeted at an increased rate.

$108 Million lost in only 6-months

The US Federal Trade Commission, in a recent 6-month period, had seen over 128,000 phone-based fraud scams that cost victims a whopping $108 Million – that's only half a year!

Staying Safe Starts with YOU!

We often assume cybercrime only happens to someone else but hackers know the easiest way to get to your organization's information is through **YOU**!

Here are some actions to stay safe.

- Be careful what you post and share online.
- Don't reuse passwords for multiple sites.
- Follow your organization's security policies and procedures.
- If something seems suspicious, always verify that it's legitimate.

In the time it took you to read this document, there were multiple cyberattacks across the globe. Make sure you stop, look, and think before you take any sort of action.

Cyber Threats Are Real:

From phishing emails disguised as trusted contacts to malicious attachments that can cripple entire systems, the risks are everywhere. Simple mistakes—like clicking a suspicious link or downloading an attachment—can expose your personal and financial information.

Our Role in Cybersecurity:

As a government entity, Douglas County is committed to safeguarding our community from cyber risks. But cybersecurity is a shared responsibility. By staying informed and cautious, you can help protect yourself and your community from online dangers.

DOUGLAS COUNTY
GEORGIA

Chapter 2

Common Online Scams and Dangers

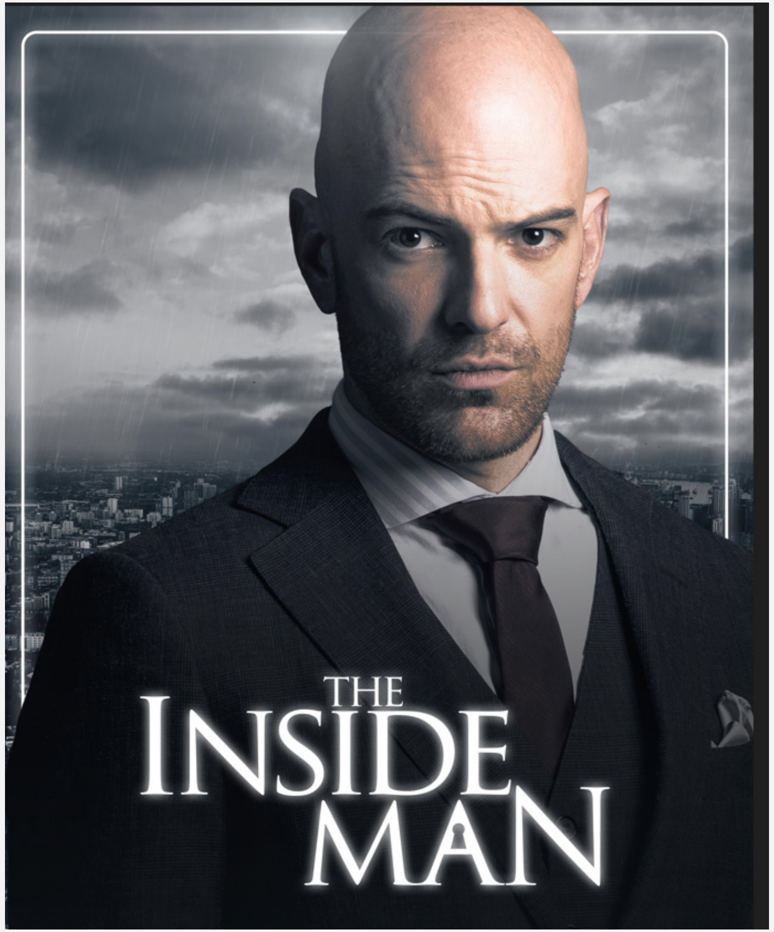
In this chapter, we'll dive into some of the most common cyber threats you may encounter and offer tips on how to avoid them.

Phishing Attacks

Phishing is a tactic where cybercriminals pose as trusted entities (such as banks or government officials) to trick you into providing sensitive information like passwords, credit card numbers, or social security numbers. Phishing emails can often look legitimate but may contain red flags like odd grammar, strange URLs, or urgent demands.

The Handler

Imagine The Handler, a phishing monster who's desperate to steal your personal information. Just like Handler's hypnotic gaze, phishing emails are designed to lure you into clicking malicious links. To defend yourself, always scrutinize unsolicited emails, especially those asking for sensitive information.



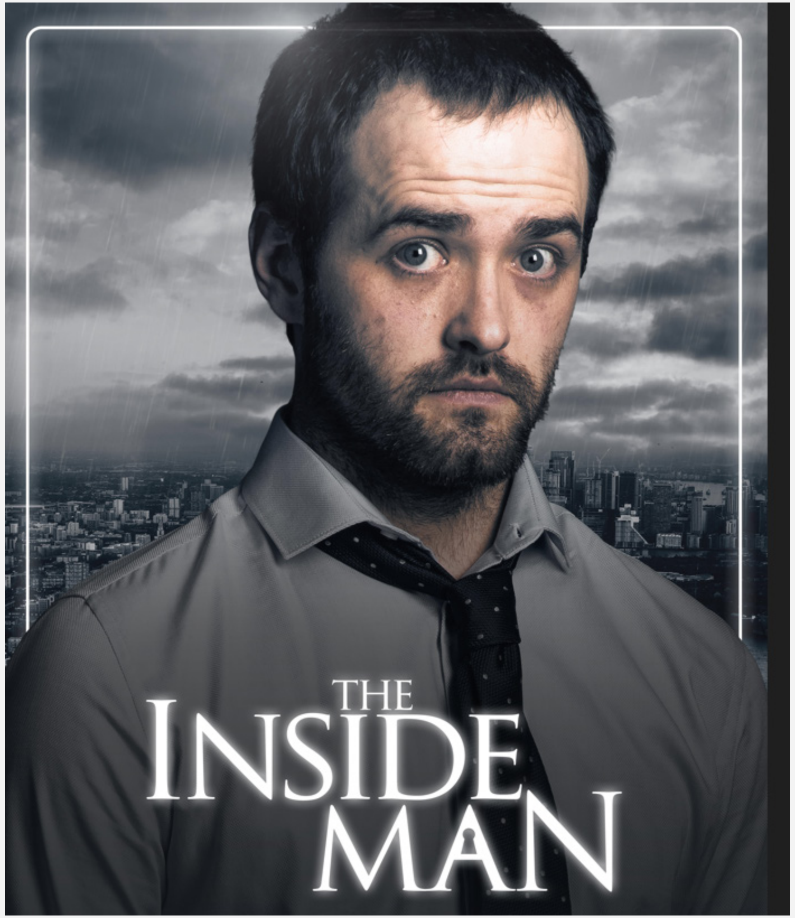
DOUGLAS COUNTY
GEORGIA

Social Engineering

This technique involves manipulating individuals into revealing confidential information. Social engineers use psychological tricks to gain trust, such as pretending to be a co-worker or authority figure.

Spoofy Mark

Spoofy Mark: Spoofy Mark, a master of disguise, represents business email compromise (BEC) scams. He tricks employees into wiring money or sharing sensitive information by posing as someone within the organization. The key to foiling Spoofy Mark is to always verify requests—especially financial ones—through a separate communication channel.



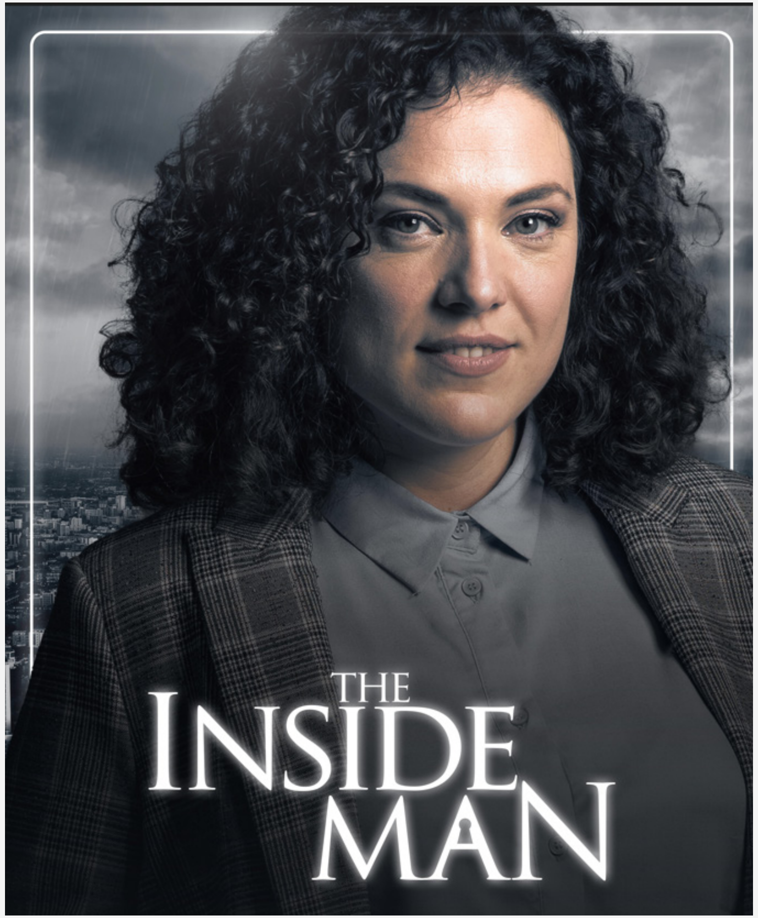
DOUGLAS COUNTY
GEORGIA

Ransomware

Ransomware is a type of malware that locks you out of your files or system until you pay a ransom. Once ransomware infects your device, it can spread quickly through networks, targeting both personal devices and larger organizations.

Fiona as Ransomewolf

The Ransomwolf lurks in innocent-looking email attachments, ready to pounce and lock your files away. The best way to fight this menace is by backing up your data regularly and ensuring that your systems are protected with up-to-date antivirus software.



DOUGLAS COUNTY
GEORGIA

Phishing Scams

What It Is: Phishing scams are one of the most widespread forms of cybercrime. Cybercriminals send fake emails pretending to be from legitimate companies or contacts, trying to steal sensitive information such as passwords, credit card details, or personal identity data.

A.J as Security Engineer

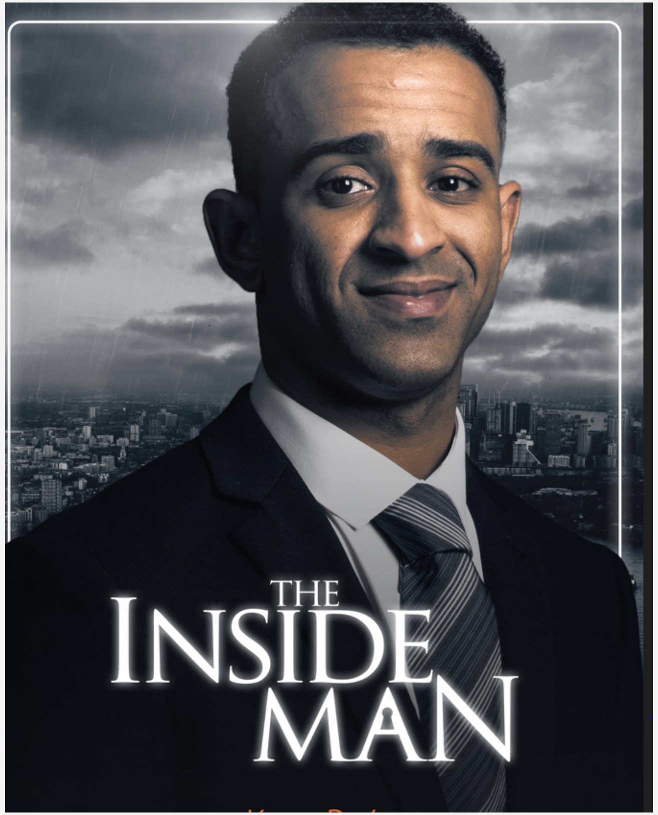
AJ's Advice: "These scams may look innocent, but don't let them fool you. Check the sender's address, and hover over any links before you click them. If the email looks urgent or asks for personal info, it's better to verify directly with the source."

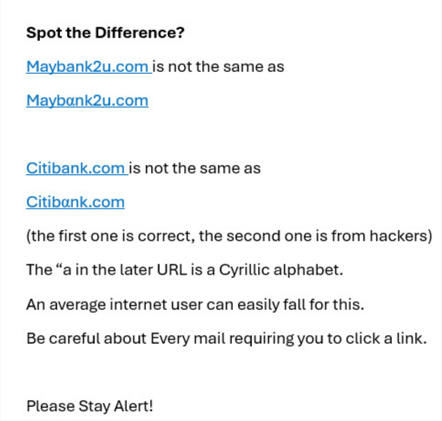
Red Flags:

- Unexpected attachments
- Grammar mistakes or unusual language
- Requests for immediate action (like password resets or financial transfers

Social Engineering Scams

What It Is: Social engineering is when an attacker manipulates you into giving away confidential information, often by pretending to be someone you trust, like a co-worker, friend, or family member.





Spot the Difference?

Maybank2u.com is not the same as

Maybаnk2u.com

Citibank.com is not the same as

Citibаnk.com

(the first one is correct, the second one is from hackers)

The "a in the later URL is a Cyrillic alphabet.

An average internet user can easily fall for this.

Be careful about Every mail requiring you to click a link.

Please Stay Alert!

DOUGLAS COUNTY
GEORGIA

AJ's Advice: "These attackers prey on human nature—especially your desire to be helpful. Always verify any unexpected requests or messages, even if it looks like it's coming from someone you know. If it feels off, trust your instincts."

Red Flags:

- Unusual requests for personal data or wire transfers
- Someone asking for help while claiming to be in urgent trouble
- Phone calls or emails from someone impersonating a trusted individual without prior notice

Online Shopping Scams

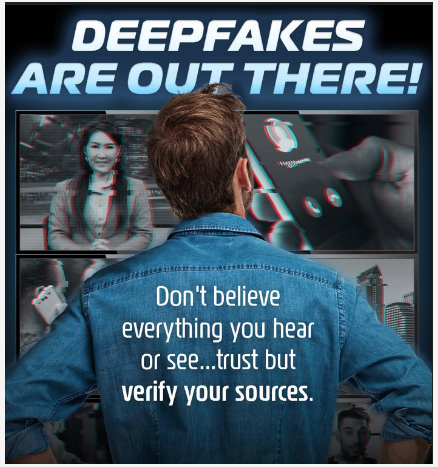
What It Is: Fake online stores or fraudulent deals may tempt you to make a purchase, but instead of delivering the goods, the scammer steals your payment information.

AJ's Advice: "If a deal seems too good to be true, it probably is. Stick to known websites, use secure payment methods, and never shop using public Wi-Fi. Always look for that padlock symbol next to the URL to make sure the site is secure."

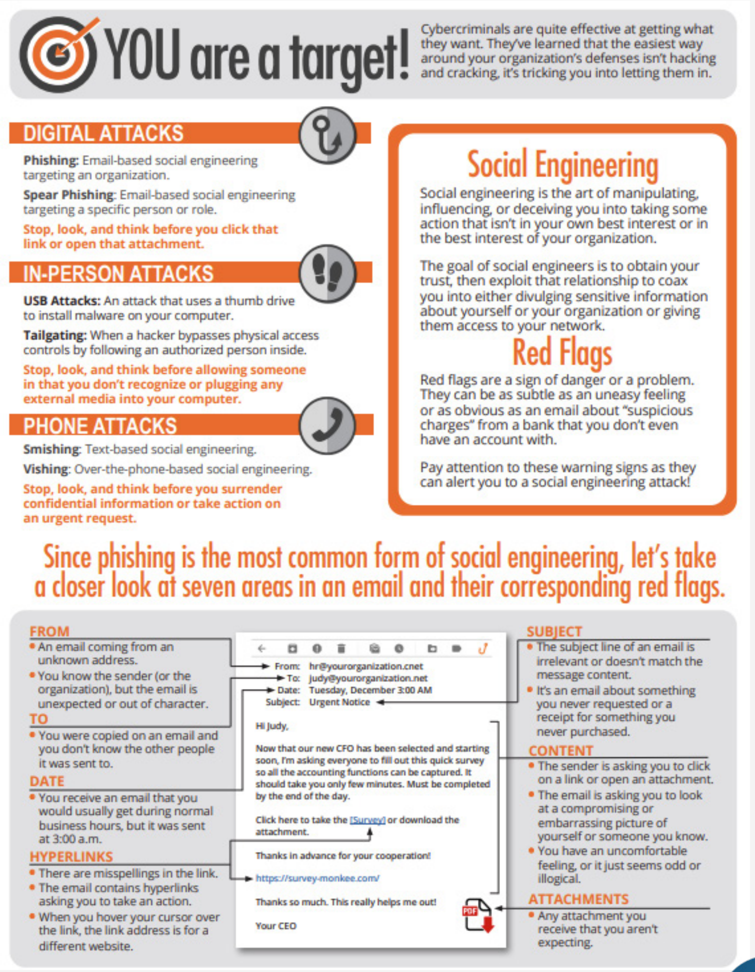
Red Flags:

- Deep discounts that are unrealistic
- Websites with minimal contact details or vague return policies
- Requests for payment via gift cards, wire transfers, or cryptocurrencies

STOP
Resist immediate action when receiving an email or text.
Title: URGENT: Your Password will expire
From: MyUniversity
Date: 12:18 AM
To: Me
Dear network user,
This email is meant to
your password will ex
in 24 hours. Follow t
update your password
Myuniversity.edu/r
Thank you
Network Security Staff
LOOK
Check for anything unusual in the message.
THINK
If something seems "phishy," report it immediately to your IT team.


DEEPFAKES ARE OUT THERE!
Don't believe everything you hear or see...trust but verify your sources.

DOUGLAS COUNTY
GEORGIA



YOU are a target!

Cybercriminals are quite effective at getting what they want. They've learned that the easiest way around your organization's defenses isn't hacking and cracking, it's tricking you into letting them in.

DIGITAL ATTACKS

Phishing: Email-based social engineering targeting an organization.

Spear Phishing: Email-based social engineering targeting a specific person or role.

Stop, look, and think before you click that link or open that attachment.

IN-PERSON ATTACKS

USB Attacks: An attack that uses a thumb drive to install malware on your computer.

Tailgating: When a hacker bypasses physical access controls by following an authorized person inside.

Stop, look, and think before allowing someone in that you don't recognize or plugging any external media into your computer.

PHONE ATTACKS

Smishing: Text-based social engineering.

Vishing: Over-the-phone-based social engineering.

Stop, look, and think before you surrender confidential information or take action on an urgent request.

Social Engineering

Social engineering is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or in the best interest of your organization.

The goal of social engineers is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or your organization or giving them access to your network.

Red Flags

Red flags are a sign of danger or a problem. They can be as subtle as an uneasy feeling or as obvious as an email about "suspicious charges" from a bank that you don't even have an account with.

Pay attention to these warning signs as they can alert you to a social engineering attack!

Since phishing is the most common form of social engineering, let's take a closer look at seven areas in an email and their corresponding red flags.

FROM

- An email coming from an unknown address.
- You know the sender (or the organization), but the email is unexpected or out of character.

TO

- You were copied on an email and you don't know the other people it was sent to.

DATE

- You receive an email that you would usually get during normal business hours, but it was sent at 3:00 a.m.

HYPERLINKS

- There are misspellings in the link.
- The email contains hyperlinks asking you to take an action.
- When you hover your cursor over the link, the link address is for a different website.

From: hr@yourorganization.cnet
To: judy@yourorganization.net
Date: Tuesday, December 3:00 AM
Subject: Urgent Notice

Hi Judy,

Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [Survey] or download the attachment.

Thanks in advance for your cooperation!

https://survey-monkee.com/

Thanks so much. This really helps me out!

Your CEO

SUBJECT

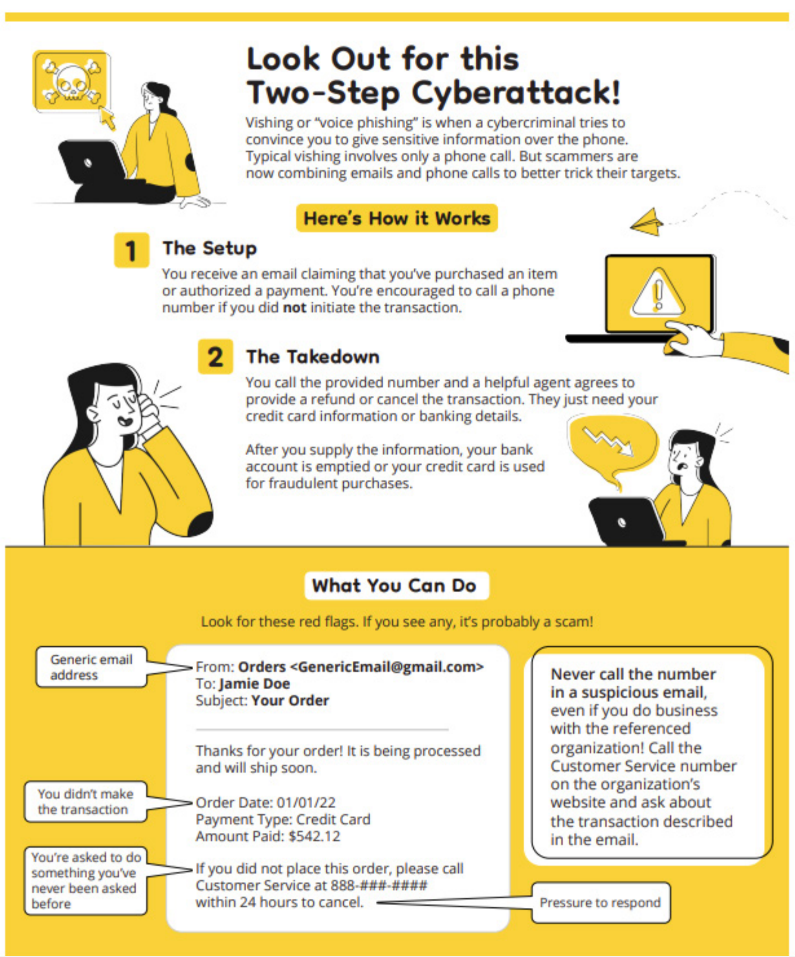
- The subject line of an email is irrelevant or doesn't match the message content.
- It's an email about something you never requested or a receipt for something you never purchased.

CONTENT

- The sender is asking you to click on a link or open an attachment.
- The email is asking you to look at a compromising or embarrassing picture of yourself or someone you know.
- You have an uncomfortable feeling, or it just seems odd or illogical.

ATTACHMENTS

- Any attachment you receive that you aren't expecting.



Look Out for this Two-Step Cyberattack!

Vishing or "voice phishing" is when a cybercriminal tries to convince you to give sensitive information over the phone. Typical vishing involves only a phone call. But scammers are now combining emails and phone calls to better trick their targets.

Here's How it Works

1 The Setup

You receive an email claiming that you've purchased an item or authorized a payment. You're encouraged to call a phone number if you did **not** initiate the transaction.

2 The Takedown

You call the provided number and a helpful agent agrees to provide a refund or cancel the transaction. They just need your credit card information or banking details.

After you supply the information, your bank account is emptied or your credit card is used for fraudulent purchases.

What You Can Do

Look for these red flags. If you see any, it's probably a scam!

Generic email address

From: **Orders <GenericEmail@gmail.com>**
To: **Jamie Doe**
Subject: **Your Order**

Thanks for your order! It is being processed and will ship soon.

You didn't make the transaction

Order Date: 01/01/22
Payment Type: Credit Card
Amount Paid: $542.12

You're asked to do something you've never been asked before

If you did not place this order, please call Customer Service at 888-###-####
within 24 hours to cancel.

Pressure to respond

Never call the number in a suspicious email, even if you do business with the referenced organization! Call the Customer Service number on the organization's website and ask about the transaction described in the email.

DOUGLAS COUNTY
GEORGIA

Chapter 3:

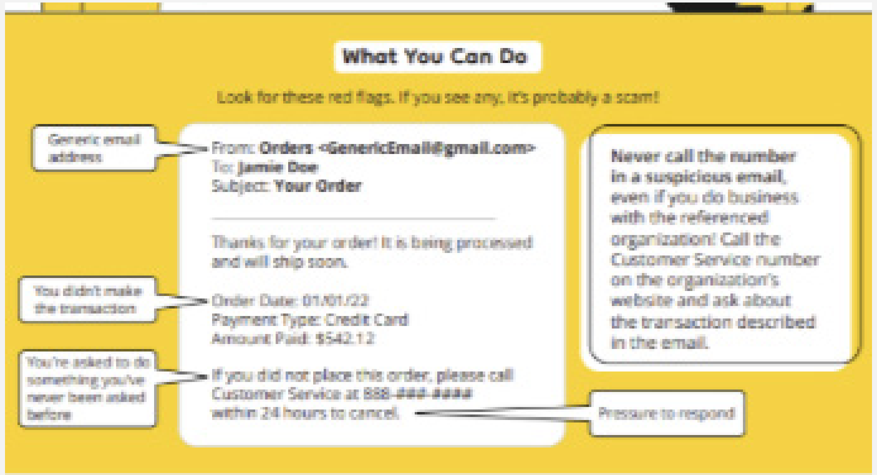
Best Practices for Online Safety

Now that you’re aware of the threats, let’s explore how to protect yourself effectively.

Email Safety

Your inbox is a primary target for cybercriminals. Follow these best practices to avoid falling victim to email scams:

- Hover over links before clicking to check if the URL looks suspicious.
- Never download attachments from unknown senders.
- Look out for urgent messages that pressure you to act immediately.
- Strong Passwords
- Passwords are your first line of defense. Make sure they’re:
- At least 12 characters long.
- A mix of upper and lower case letters, numbers, and symbols.
- Different for each account. Consider using a password manager to store and create secure passwords.



What You Can Do

Look for these red flags. If you see any, it's probably a scam!

From: **Orders <GenericEmail@gmail.com>**
To: **Jamie Doe**
Subject: **Your Order**

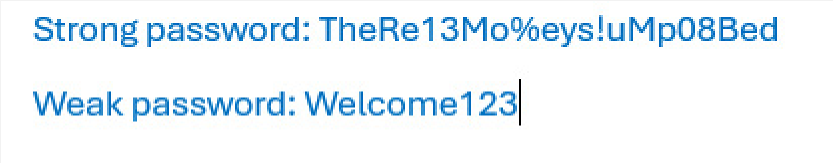
Thanks for your order! It is being processed and will ship soon.

Order Date: 01/01/22
Payment Type: Credit Card
Amount Paid: $542.12

If you did not place this order, please call Customer Service at 888-###-#### within 24 hours to cancel.

Never call the number in a suspicious email, even if you do business with the referenced organization! Call the Customer Service number on the organization's website and ask about the transaction described in the email.

Generic email address
You didn't make the transaction
You're asked to do something you've never been asked before
Pressure to respond



Strong password: TheRe13Mo%eys!uMp08Bed

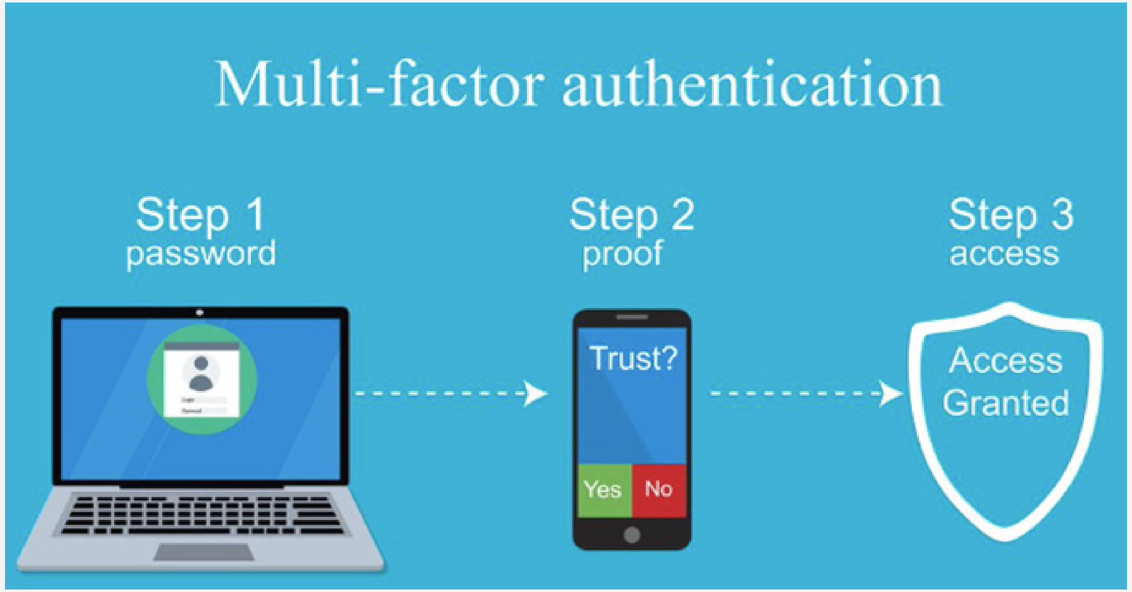
Weak password: Welcome123

DOUGLAS COUNTY
GEORGIA

Multi-Factor Authentication (MFA)

Enable MFA wherever possible. It adds an extra layer of security by requiring not just your password but also something you have (like a phone app) or something you are (like a fingerprint).

Regular Updates - Cybercriminals often exploit outdated computers and software



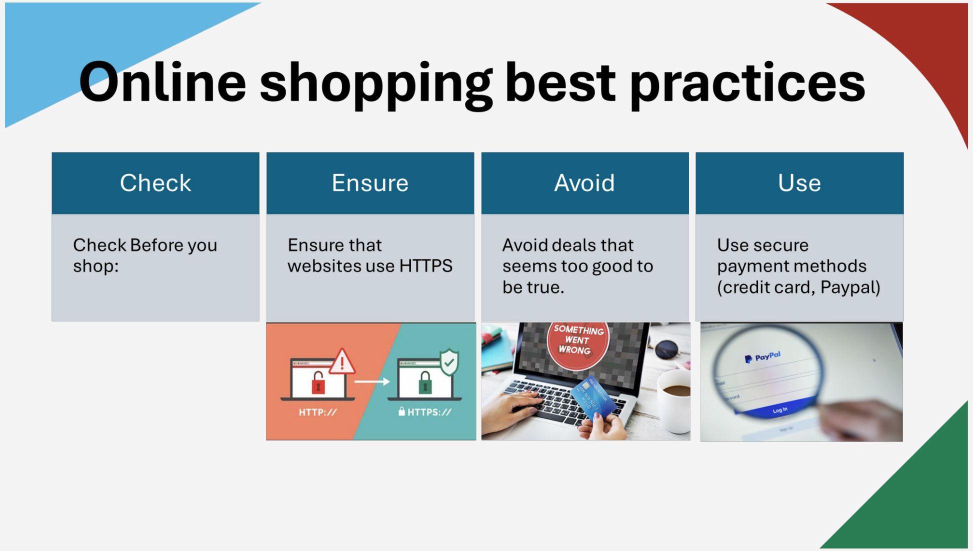
DOUGLAS COUNTY
GEORGIA

Chapter 4:

Safe Online Shopping Tips

Online shopping is convenient, but it also exposes you to certain risks. Follow these tips for a secure shopping experience:

Shop from trusted websites: Look for "https" in the URL and a padlock symbol.
Avoid public Wi-Fi for online purchases; if you must, use a VPN.
Use credit cards instead of debit cards for extra protection against fraud.
Beware of deals that seem too good to be true—they probably are.



Online shopping best practices

Check	Ensure	Avoid	Use
Check Before you shop:	Ensure that websites use HTTPS	Avoid deals that seems too good to be true.	Use secure payment methods (credit card, Paypal)

HTTP://
HTTPS://
SOMETHING WENT WRONG
PayPal

DOUGLAS COUNTY
GEORGIA

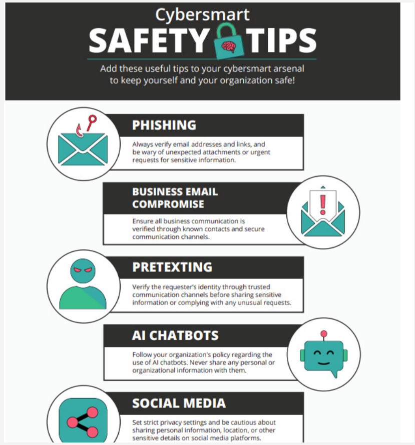
Chapter 5

Handling Suspicious Activity

No matter how careful you are, there's always a chance that you might encounter a cyber threat. Here's what to do if something seems off:

- Phishing email: Do not respond. Report it to your email provider or IT team.
- Suspicious charge on your credit card: Contact your bank immediately to freeze the card.
- Possible malware infection: Disconnect from the internet and run an antivirus scan.

Douglas County also provides local support for reporting cyber incidents. If you suspect a cybercrime, visit our [local cyber support portal] for help.



Cybersmart

SAFETY TIPS

Add these useful tips to your cybersmart arsenal to keep yourself and your organization safe!

PHISHING

Always verify email addresses and links, and be wary of unexpected attachments or urgent requests for sensitive information.

BUSINESS EMAIL COMPROMISE

Ensure all business communication is verified through known contacts and secure communication channels.

PRETEXTING

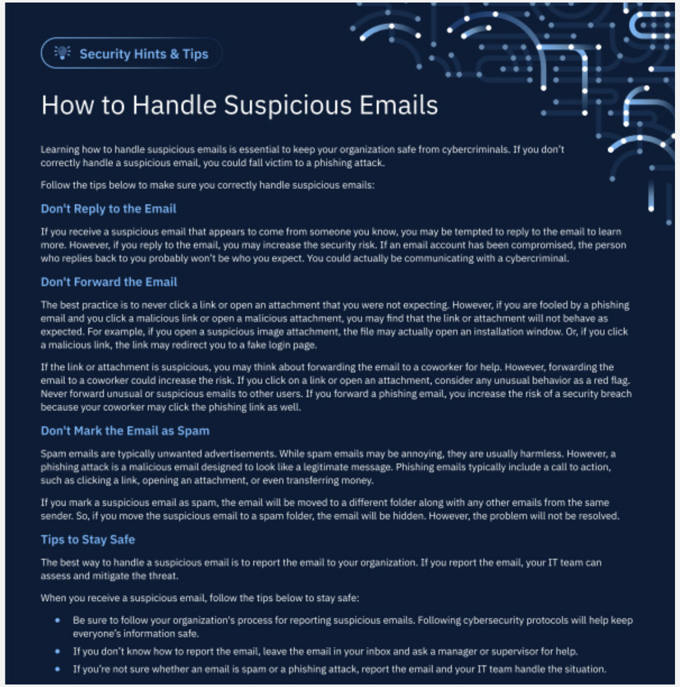
Verify the requester's identity through trusted communication channels before sharing sensitive information or complying with any unusual requests.

AI CHATBOTS

Follow your organization's policy regarding the use of AI chatbots. Never share any personal or organizational information with them.

SOCIAL MEDIA

Set strict privacy settings and be cautious about sharing personal information, location, or other sensitive details on social media platforms.



Security Hints & Tips

How to Handle Suspicious Emails

Learning how to handle suspicious emails is essential to keep your organization safe from cybercriminals. If you don't correctly handle a suspicious email, you could fall victim to a phishing attack.

Follow the tips below to make sure you correctly handle suspicious emails:

Don't Reply to the Email

If you receive a suspicious email that appears to come from someone you know, you may be tempted to reply to the email to learn more. However, if you reply to the email, you may increase the security risk. If an email account has been compromised, the person who replies back to you probably won't be who you expect. You could actually be communicating with a cybercriminal.

Don't Forward the Email

The best practice is to never click a link or open an attachment that you were not expecting. However, if you are fooled by a phishing email and you click a malicious link or open a malicious attachment, you may find that the link or attachment will not behave as expected. For example, if you open a suspicious image attachment, the file may actually open an installation window. Or, if you click a malicious link, the link may redirect you to a fake login page.

If the link or attachment is suspicious, you may think about forwarding the email to a coworker for help. However, forwarding the email to a coworker could increase the risk. If you click on a link or open an attachment, consider any unusual behavior as a red flag. Never forward unusual or suspicious emails to other users. If you forward a phishing email, you increase the risk of a security breach because your coworker may click the phishing link as well.

Don't Mark the Email as Spam

Spam emails are typically unwanted advertisements. While spam emails may be annoying, they are usually harmless. However, a phishing attack is a malicious email designed to look like a legitimate message. Phishing emails typically include a call to action, such as clicking a link, opening an attachment, or even transferring money.

If you mark a suspicious email as spam, the email will be moved to a different folder along with any other emails from the same sender. So, if you move the suspicious email to a spam folder, the email will be hidden. However, the problem will not be resolved.

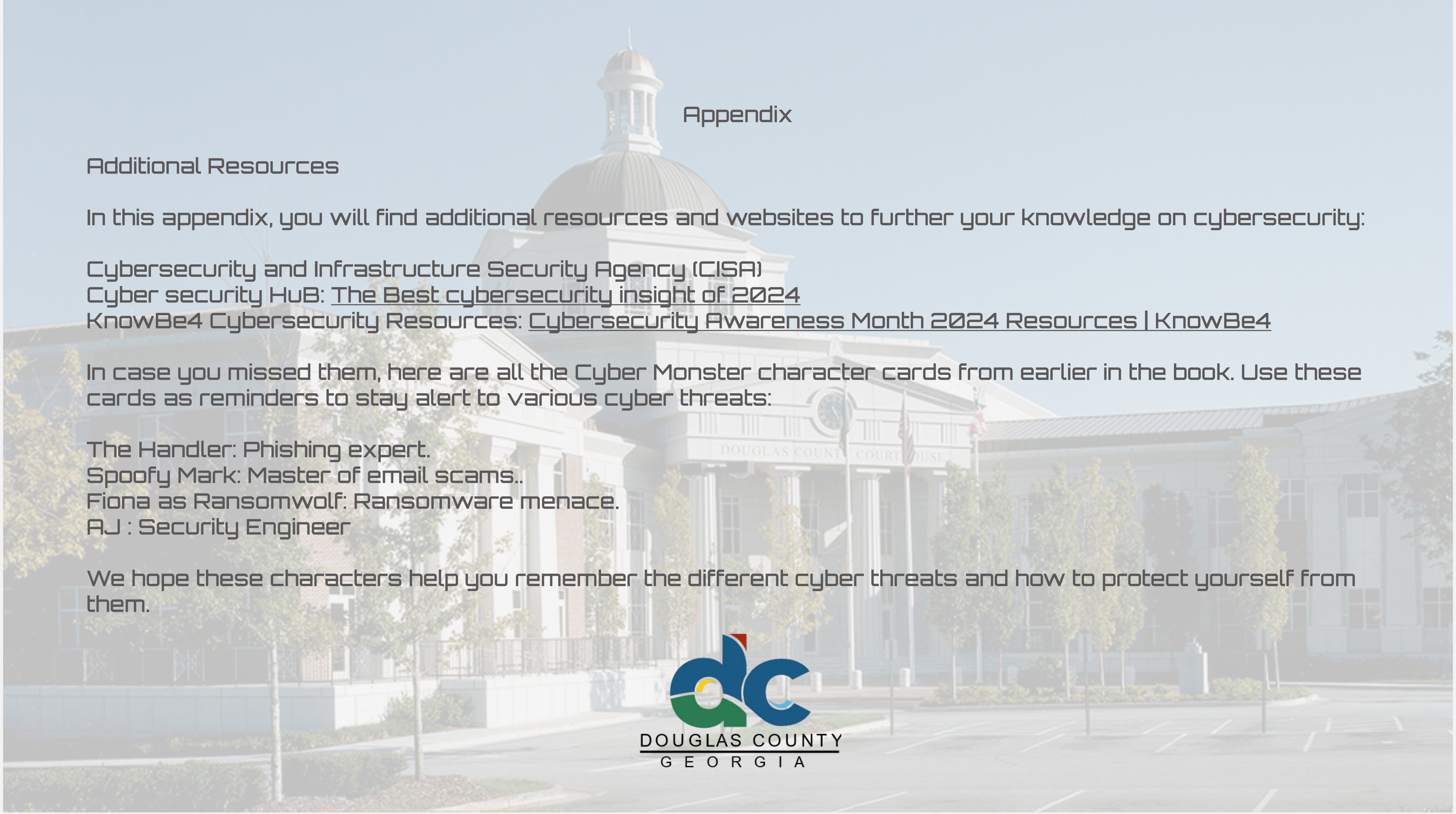
Tips to Stay Safe

The best way to handle a suspicious email is to report the email to your organization. If you report the email, your IT team can assess and mitigate the threat.

When you receive a suspicious email, follow the tips below to stay safe:

- Be sure to follow your organization's process for reporting suspicious emails. Following cybersecurity protocols will help keep everyone's information safe.
- If you don't know how to report the email, leave the email in your inbox and ask a manager or supervisor for help.
- If you're not sure whether an email is spam or a phishing attack, report the email and your IT team handle the situation.

DOUGLAS COUNTY
GEORGIA



Appendix

Additional Resources

In this appendix, you will find additional resources and websites to further your knowledge on cybersecurity:

Cybersecurity and Infrastructure Security Agency (CISA)
Cyber security HuB: The Best cybersecurity insight of 2024
KnowBe4 Cybersecurity Resources: Cybersecurity Awareness Month 2024 Resources | KnowBe4

In case you missed them, here are all the Cyber Monster character cards from earlier in the book. Use these cards as reminders to stay alert to various cyber threats:

The Handler: Phishing expert.
Spoofy Mark: Master of email scams..
Fiona as Ransomwolf: Ransomware menace.
AJ : Security Engineer

We hope these characters help you remember the different cyber threats and how to protect yourself from them.

DOUGLAS COUNTY
GEORGIA

THE HANDLER

Maurice is the sinister "Handler" who sends Mark in to steal sensitive business information from Khromacom. He's the voice on the phone sending dread into the young hacker's heart and the stranger hiding in plain sight. Maurice is a ninja-level social engineer who can flip from Texas businessman to hipster waiter in a heartbeat. A mysterious figure from Mark's past, Maurice's actions never cease to surprise.

MARK

Mark comes from a world of secrets and lies. As "the inside man" for a mysterious 'Handler' pulling the strings, he is on a mission to take down Khromacom, regardless of the people who work there. Forced to confront his own beliefs and the ghosts from his past, we find him developing a conscience as he builds relationships with colleagues, combating insider threats and outsider attacks.

FIONA

Fiona is the voice of humanity at Khromacom when all seems to be going haywire. She's grounded and thoughtful and brings insights on human nature that lay bare the collateral damage done by hackers. With an impressive hunger to learn, Fiona is one to keep an eye on. It seems fate has decreed her adventures with Mark and AJ at Khromacom may be just the beginning.

AJ

AJ is a friendly, funny, unstoppable security dynamo with a deep love of all things tech. He's lucked into the job of his dreams, working in security, alongside Mark Shepherd. AJ is Mark's conscience and keeps him grounded, even when cyber threats abound. AJ is relentlessly upbeat and can be guaranteed to provide comic relief, whether that's speed-eating marshmallows or updating his followers on YouTube - all 57 of them.

REMEMBER:

Cybersecurity is everyone's responsibility. By staying informed, recognizing the signs of online scams and practicing safe online habits, we can protect ourselves and our community from digital threats. Whether its avoiding phishing emails, securing your passwords, or shopping online with caution these small steps can make a difference.

DOUGLAS COUNTY
GEORGIA