

unmasked

A Scam-Smart Workshop for Our Community

UNMASKEDNJ.COM

DID YOU KNOW?

85% of people posting puppy photos are actually trying to scam you



"Coronavirus Pandemic Coincides With Spike in Online Puppy Scams," Sophos, 2020

How can we stop these evil puppies?



Our Friends for Today



01

Sam



02

Martha



03

Jerry



04

Lisa



05

Luke



06

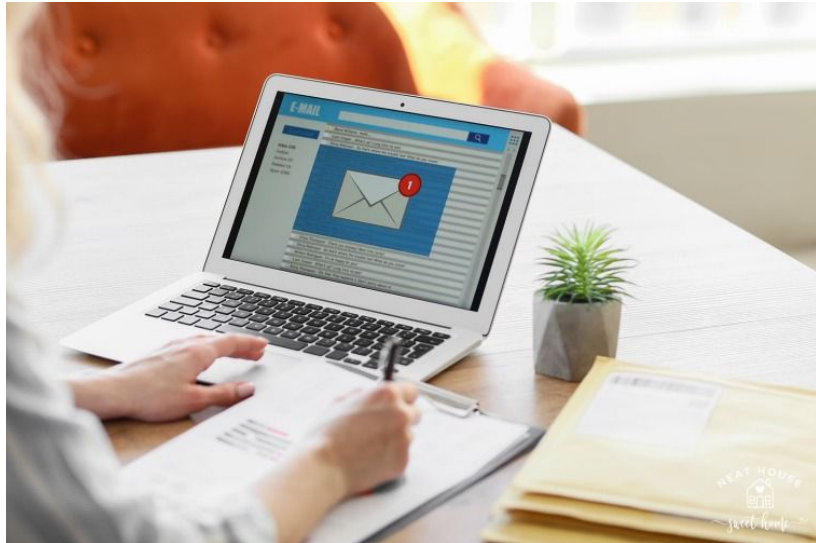
David



MEET

Sam

STORY



Sam, a retired teacher, checks her emails every morning. One morning, Sam received an email that read, "URGENT: Your account will be locked if you don't act now!"

STORY



Worried, Sam clicked the link in the email. It took her to a page that looked like her bank's website. It asked for her username, password, and even her credit card number to "verify her account." Sam hesitated. Something felt off, but the warning about her account being locked made her nervous.

STORY



Before she typed in her details, she remembered her friend's important advice: "Real companies never ask for your password or sensitive details through email." Sam closed the email and called her bank directly. The bank confirmed it was a scam. Relieved, Sam deleted the email and learned to be extra cautious.

How Sam Protected Herself



Spotting Red Flags

She noticed the email sounded urgent and the link in it was strange - "www.bank-secure123.com" instead of her actual bank's website.



Staying Safe

Instead of clicking links in the email, Sam called her bank using the number on her official bank statement to confirm.



Deleting the Threat

After verifying it was a phishing attempt, Sam deleted the email and didn't share any information.

CONCEPT

Phishing



Phishing is a cyberattack where scammers trick individuals into providing sensitive information, like passwords or credit card details, by posing as a trusted entity, often through fake emails or websites.



SCENARIO



You've just received an email claiming to be from your bank. It says:

"Your account will be locked in 24 hours unless you confirm your personal details. Click here to verify: www.bank-secure123.com"

What Should YOU Do?

- A** Click the link and log in quickly to save your account.
- B** Call your bank directly using the number on your bank statement.
- C** Reply to the email asking if it's real.



CORRECT ANSWER

B.

Call your bank directly!

Never click on suspicious links or reply to emails asking for personal information. Always verify by contacting your bank using their official number.



MEET

Martha

STORY



Martha was having tea when she got a call from "John at Microsoft," warning her about a fast-spreading virus on her computer.

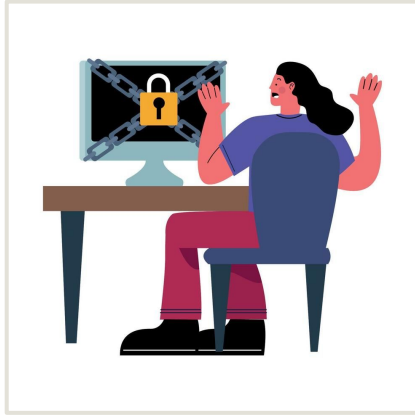
Panicked, she followed his instructions to install a program for a "fix." He then demanded a \$200 payment via gift cards.

STORY



Wanting to protect her files, she complied,
bought the cards, and shared the codes.
John thanked her and hung up.

The Aftermath



The next day, Martha tried to use her computer, but it was locked. A message popped up demanding more money to unlock it.



Panicking, she called her son, who immediately knew what had happened. "Mom, you've been scammed! Microsoft doesn't call people like that. We need to contact the bank and file a report right away."



Together, they reported the scam to her bank and the police. Unfortunately, the money she sent through gift cards was gone for good.

What Martha Learned



With the help of her son, Martha managed to resolve the situation, but she still lost money spent on gift cards. From this experience, Martha has learned:

- ✓ It's okay to pause and double-check before following instructions from unexpected callers.
- ✓ Big companies like Microsoft won't ask for gift cards or call out of the blue.
- ✓ Talking to a trusted family member can help make things clearer and safer.
- ✓ If something feels off, it's always a good idea to report it. There's help available.

Tell the FTC:

ReportFraud.ftc.gov

#stopscams

Did someone tell you to buy a gift card and give them the numbers?

That's a scam.

Report it to the gift card company.

Ask for your money back.



CONCEPT

Scam Calls



Receiving a call from someone claiming to be from a well-known company might seem serious, but it could be a scam.

These callers often pretend there's a problem with your computer or account and ask for money or personal information. In reality, they're just trying to trick you.



SCENARIO



You're enjoying a quiet afternoon when the phone rings. The caller says,

"This is Mike from your electricity company. There's an unpaid bill on your account, and your power will be shut off in an hour unless you pay immediately. To avoid disconnection, you can pay right now using a prepaid card or wire transfer."

The idea of losing electricity makes you nervous.

How should you respond?

- A** Follow their instructions and pay quickly to avoid losing power.
- B** Ask them for their name and employee ID to verify the call.
- C** Hang up and call your electricity company using the number on your bill.



CORRECT ANSWER

C.

Hang up and call your electricity company using the number on your bill.

Utility companies **WILL NOT** demand immediate payment or threaten disconnection without prior written notice. Always verify using their official contact information.



MEET

Jerry

STORY



One sunny afternoon, Jerry sat down to check his email. Logging in was always quick since he used the password, "123456," and it was easy to remember. Jerry used the same password for everything: email, shopping, even his bank account.

Later that evening, Jerry's phone buzzed with an alarming message:

"Your account was accessed from a new location. If this wasn't you, please reset your password immediately."

STORY



Feeling helpless, Jerry called a tech-savvy friend, Sarah, who quickly explained: "Jerry, your password was way too simple, and you used it everywhere! Hackers guessed it easily and used it to break into all your accounts."

Jerry panicked and logged into his email, only to find strange messages he hadn't sent.

Worse, when Jerry tried to log in to his shopping account, his password didn't work anymore.

What Jerry Learned



Sarah helped Jerry fix the situation, but it was a lot of work. They had to:

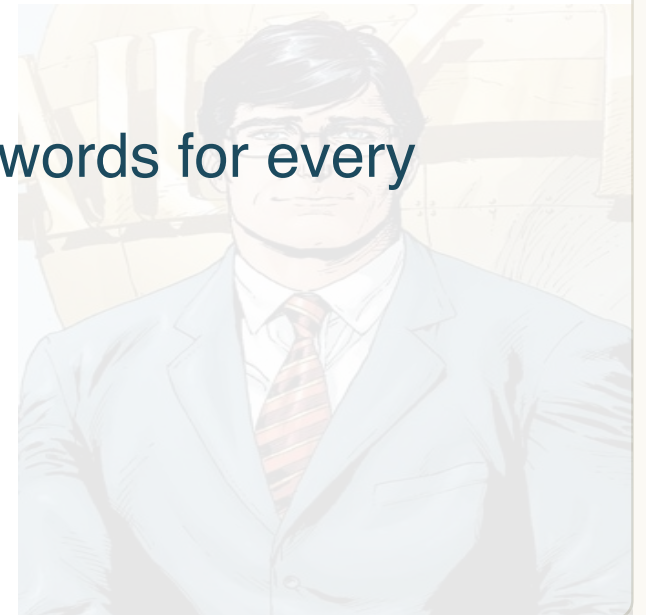
- ✓ Reset passwords on every account.
- ✓ Contact his bank to report suspicious activity.
- ✓ Set up stronger passwords with a mix of letters, numbers, and symbols, like "@Str0ng#P@ssw0rd!"





Jerry learned the hard way that simple passwords are an open door for hackers.

From that day forward, Jerry used unique, complex passwords for every account and kept them safe with a password manager.



CONCEPT



Weak/Repeated Passwords

Weak passwords are passwords with common patterns/information (ex: 123456, password123).

Using the same password exponentially increases the risk of hackers taking your important personal information.



SCENARIO



Chris sets his password to "chris123" for his email account.

Why is "chris123" a weak password?

- A** It's too short and lacks complexity.
- B** It includes a name that's easy to guess.
- C** It doesn't have special characters like @, #, or \$.
- D** All of the above.



CORRECT ANSWER

D.

All of the above!

✓ It's too short, making it easy for hackers to guess.

✓ It includes a common name, which is predictable.

✓ It lacks complexity, like uppercase letters, numbers, and special characters.

Password Game

We will be handing out slips of paper and pens for you to write with. We will be asking you to write a strong, complex password on the piece of paper.



Don't just write random letters and characters, the password has to be easy to remember as well!



Also, DO NOT write a password that you currently use.

Once you've written your password, fold the paper and write your name so we can come around and collect them.

We will be ranking the passwords, and the best password will be chosen at the end of our presentation, and you will receive a prize!



MEET

Lisa

STORY



Lisa loves playing online games and browsing the internet in her free time. One day, as she was scrolling through a website, a flashy pop-up appeared:

"Congratulations! You've won \$1,000! Click here to claim your prize!"

Excited by the idea of winning, Lisa clicked the link. The website asked her to download a file to "verify her prize." Without thinking, she downloaded it and waited for her winnings.

STORY



shutterstock.com • 1722602176

Instead of getting \$1,000, Lisa noticed her computer started acting strangely. It slowed down, random ads starting popping up everywhere, and her browser kept opening weird websites she didn't recognize.

Panicked, she called her tech-savvy friend, Emma. Emma listened to Lisa's story and sighed, "Lisa, you downloaded malware! That file wasn't safe. It can steal your information or mess up your system!"

What Lisa Learned



Emma helped Lisa fix her computer by running an antivirus program, but Lisa had learned her lesson the hard way. She now knows:

- ✓ Don't click on flashy ads or pop-ups, especially ones promising prizes.
- ✓ Be cautious when downloading files, especially from unknown websites.
- ✓ Always keep antivirus software installed and updated to catch malware before it causes problems.



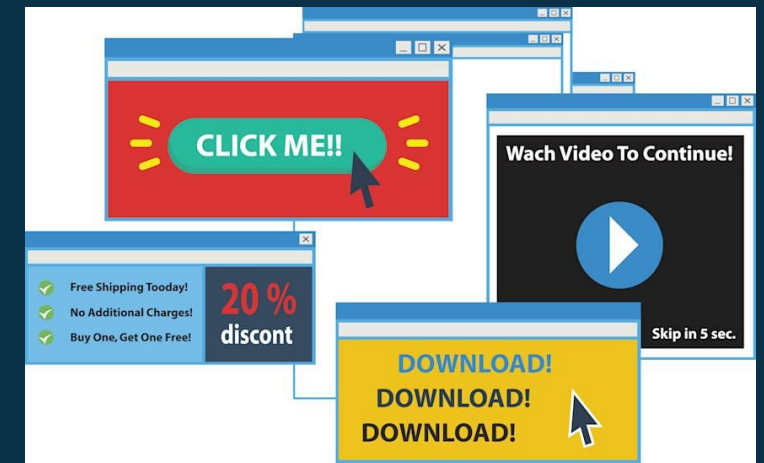
CONCEPT

Viruses & Malware



Viruses and malware are software that can harm your computer or steal your information. A virus spreads by attaching itself to files and sharing with others.

Malware is any harmful software, like viruses, or programs that lock your files or spy on you. It's important to protect your computer. Avoid clicking random pop-ups or accepting "free" cash



SCENARIO



Jeremy is googling the answers to his homework.

A pop-up appears:

"Quick! You have 60 seconds to claim a free Iphone 16!"

What should Jeremy do?

- A** CLAIM THE FREE iPhone!!
- B** Close out the pop up
- C** Panic and quickly click on the pop up



CORRECT ANSWER

B.

Close out the pop up

Do NOT click any links or downloads. The free iPhone is a virus in disguise. Calmly close out the pop up and avoid danger!



MEET

Luke

STORY



Luke is at his local Starbucks. He is sipping on his matcha latte, about to make an online purchase after he checks all of his recent emails.

He opens his laptop to access the public free Wifi and sees "Starbucks_Free_WiFi", and he clicks on it.

STORY



Someone has hacked the Starbucks wifi, and is able to see everything that happens on the screen of those who connect to it!

Luke, unknowing of the hacker's infiltration of the network, connects to it. As he logs into his email and enters all his credit card details to make the purchase, the hacker captures all his information through the WiFi.

CONCEPT



OH NO!

Luke's data, including his email credentials and credit card information, is now in the hands of a HACKER. This could lead to identity theft, unauthorized purchases, or even access to sensitive accounts.



What YOU Need to Do



In order to avoid ourselves from ending up in Luke's situation, there are a some precautions that we can take:

1

Verify the Network
Name

2

Use a Virtual Private
Network (VPN):

3

Avoid Sensitive
Transactions

CONCEPT

Public Wi-Fi Risks



Using free Wi-Fi at a coffee shop or airport might seem convenient, but hackers can spy on what you're doing.

They might steal your passwords, emails, or even financial information.





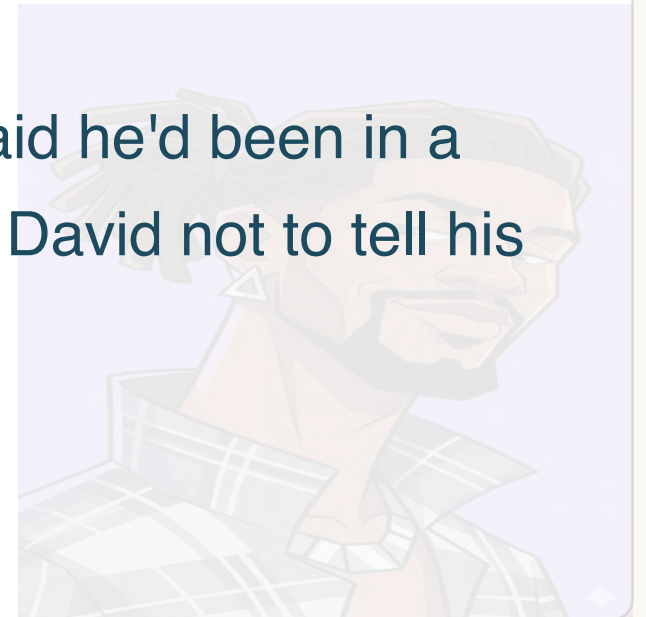
MEET

David



It was 9 PM when David's phone rang. "Grandpa, I'm so sorry, I didn't know who else to call."

It sounded exactly like Ethan, his grandson. The voice said he'd been in a car accident and needed money right away, and begged David not to tell his parents.





1

David's heart was racing. He didn't stop to think it through. He grabbed his keys and drove straight to the store.

2

At the register, David bought \$500 in gift cards and called the number back with shaking hands, reading off each code as he was told. The voice on the phone thanked him and said everything would be taken care of.

The Aftermath



David didn't sleep that night, waiting for Ethan to call and say he was okay. Ethan never ended up calling.

The next morning, his daughter called instead, confused about why he sounded so shaken. Ethan had been in class the entire evening and had never called anyone. The voice on the phone, the crying, the panic, all of it, had been generated by AI trained to sound exactly like his grandson. The \$500 was gone, and there was no getting it back.

What David Learned



David reported the scam to his bank and the police, but the gift card money couldn't be traced or recovered. Looking back, he realized how much the urgency and the crying had clouded his judgment.

From this experience, he learned:



A voice alone isn't proof of who's calling, even if it sounds exactly right.



Real emergencies can be checked by calling the person back on a number you already have.



A request to keep something secret from the rest of the family is a warning sign.



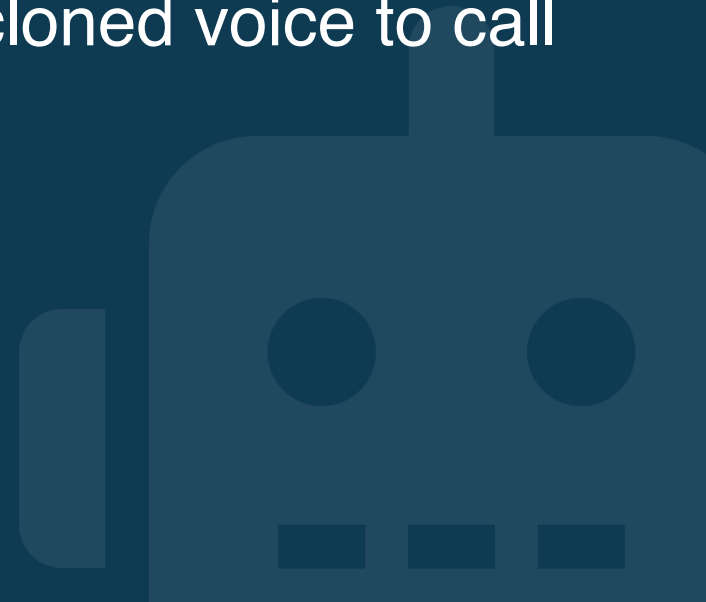
It's always worth reporting, even after money has been sent.

CONCEPT



AI Voice Cloning

AI voice cloning is when scammers use artificial intelligence to copy a person's voice from a short recording, sometimes only a few seconds, often pulled from a video posted online. They use the cloned voice to call a family member and ask for money right away.



SCENARIO



It's late at night when you get a call from a number you don't recognize. The voice sounds exactly like your grandchild, crying, saying they've been in an accident and need money right away. They beg you not to tell the rest of the family.

What should you do?

- A** Wire the money right away.
- B** Hang up and call your grandchild back on the number you already have for them.
- C** Ask them to prove it's really them by saying their own name.



CORRECT ANSWER

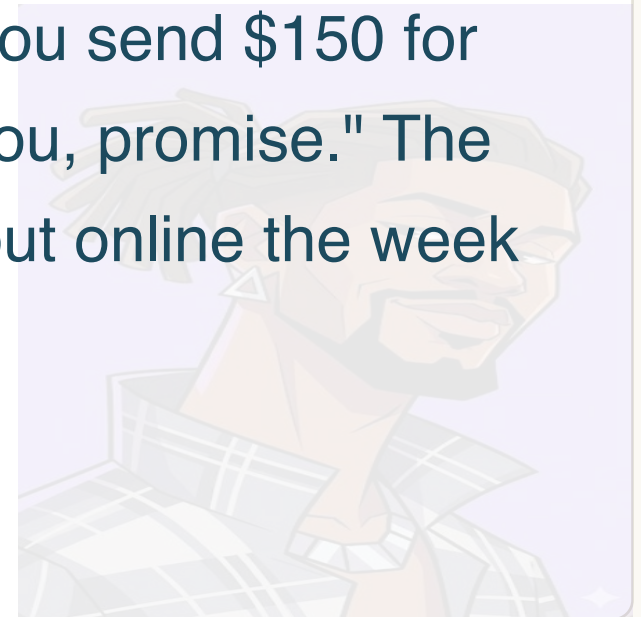
B.

Hang up and call your grandchild back on a number you already have.

AI can copy a real voice closely enough that hearing it is no longer proof of who's calling. A request for secrecy paired with a request for money, especially late at night, is a warning sign. Always verify independently before sending anything.



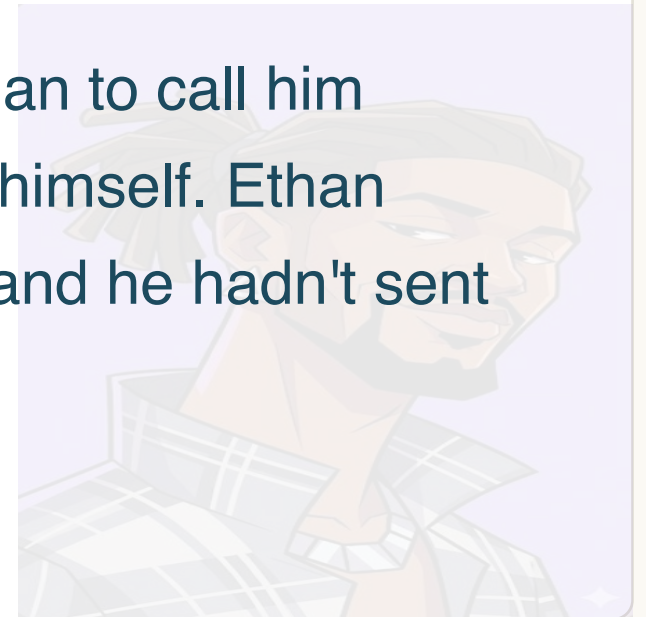
A few weeks later, David was scrolling through old photos when his phone buzzed with a text from what looked like Ethan's number. "Hey Grandpa, lost my phone, texting from a friend's. Can you send \$150 for a bus ticket home? I'll explain everything when I see you, promise." The message even mentioned a trip Ethan had posted about online the week before.





This time David paused. He thought back to the night he'd lost \$500 to a voice that wasn't really Ethan's.

Instead of sending the money, he texted back asking Ethan to call him directly. No call came. David dialed Ethan's real number himself. Ethan picked up, confused, he was home, his phone was fine, and he hadn't sent any message asking for money.



CONCEPT



AI Text Scams

Scammers can use artificial intelligence to read someone's public posts and write a text in their style, mentioning real details to sound convincing. A text that sounds exactly like someone you know is not proof it's them, especially if it's asking for money.

SMS

IMPORTANT

Americans 60 and older reported losing nearly \$2.4 billion to scams in 2024, roughly four times what it was in 2020. And that's only what got reported.

The FTC estimates the true cost to older adults was somewhere between \$10 billion and \$81 billion, because a lot of fraud just never gets reported. Most of these scams don't even take a hacker. They rely on fake texts, a call that sounds like someone you love, and just a few moments of someone panicking.

Key Takeaways

1

Cybersecurity protects you from scams that could lead to loss of money and private information.

2

There are many ways scammers try to get your information.

3

Do not be so trusting with emails and messages; especially if they have a link and ask for personal information.

4

Having diverse and strong passwords help prevent hackers from stealing accounts. Apps or notes can be used to keep track of the long passwords.

5

Using antivirus software will help as another layer of defense. Still be wary that antivirus programs are not perfect and may not catch all malware.

Thanks!



unmasknj@gmail.com



+1 (929) - 575 - 8416



unmaskednj.com

SOCIALS

"unmaskednj" on all platforms



unmasked