

9th-12th Education

April is National Financial Literacy Month, which is designed to create awareness about the importance of personal financial education. Over the next 4 weeks, we will be exploring different financial education topics with specific age-minded activities and links, designed for your use at home.

This week, our topic is Online Awareness. We know that 8 out of 10 teens are spending most of their time online chatting with friends on social media or in games. While it can be very entertaining and engaging, it also requires a good understanding of how to protect yourself from online scams and fraudsters.

Most people are concerned about the amount of personal information that is available online, and we don't want to be vulnerable to scammers. We have included some great websites to bookmark and articles for you to review, giving you some helpful information to keep yourself aware of online fraud and scams. There are some fun activities attached as well!

Websites for Current Scams and Online Security (bookmark these!)

<https://fraud.org/>

[Scam Alerts | FTC Consumer Information](#)

Articles, Videos and Games for Online Security

<https://www.internetmatters.org/advice/14plus/#together>

[OnGuardOnline | FTC Consumer Information](#)



Fraud and Identity Theft Definitions

- **Data breach**: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. Someone who gets the data might use it for identity theft.
- **Elder financial exploitation**: The illegal or improper use of an older adult's funds, property, or assets by family members, caregivers, friends, or strangers who gain their trust.
- **Foreclosure relief scam**: Scheme to take your money or your house often by making a false promise of saving you from foreclosure; includes mortgage loan modification scams.
- **Identity theft**: Using your personal information — such as your name, Social Security number, or credit card number — without your permission.
- **Imposter scam**: An attempt to get you to send money by pretending to be someone you know or trust, like a sheriff; local, state, or federal government employee; a family member; or charity organization.
- **Mail fraud scam**: Letters that look real but contain fake promises. A common warning sign is a letter asking you to send money or personal information now to receive something of value later.
- **Phishing scam**: When someone tries to get you to give them personal information, such as through an email or text message, often by impersonating a business or government agency. This can be thought of as “fishing for confidential information.”
- **Spoofing**: When a caller disguises the information shown on your caller ID to appear as though they are calling as a certain person or from a specific location.
- **Tax-related identity theft**: When someone steals your Social Security number to file a tax return claiming a fraudulent refund; may also be called tax-filing-related identity theft.
- **Wire transfer fraud**: Tricking someone into wiring or transferring money to steal from them. One common example of a wire transfer fraud is the “grandparent scam.” This is when a scammer posing as a grandchild or a friend of a grandchild calls to say they are in a foreign country, or in some kind of trouble, and need money wired or sent right away.

Fraud and Identity Theft Scenarios

Match each scenario with a **word bank** term at the bottom of the page.

1. You receive an email that encourages you to click a link and enter personal information, including your Social Security number and bank account number. The email looks official, but the sender's email address seems odd.
2. You contact the IRS to ask for more time to file your taxes, but you find out that someone has already filed a tax return in your name.
3. You receive a letter from an unknown company with a message that you've won a cash prize. To claim your prize, you'll need to send them your bank account information so they can deposit the money into your account. The company then uses your bank account information to take money from you.
4. Your caller ID shows that a local number associated with the high school in your town is calling you. You answer and the person calling says they're raising money for a local sports tournament. You soon realize the caller is not actually with the school.
5. You get a call from someone raising money for a charity. They ask you to wire money immediately because they have a critical and urgent humanitarian need. They get annoyed when you ask them for more information.
6. You get a call from someone claiming to be with the sheriff's office. They say they need your personal information to update their neighborhood records. You quickly recognize they're an imposter and not actually who they claim to be.
7. Someone pretending to be you used your name and personal information to borrow money to purchase a car.
8. Your grandmother has a neighbor who has gained her trust but has been secretly taking money from her bank account.
9. A hacker stole information from your credit card company, including your personal data, and used it to charge purchases.
10. You receive a letter saying that your house is in foreclosure and will be taken by the bank unless you mail a check and your personal information immediately. You know you've been paying your mortgage on time.

Word Bank:

Foreclosure relief Scam

Phishing scam

Mail fraud scam

Elder financial exploitation

Imposter scam

Data breach

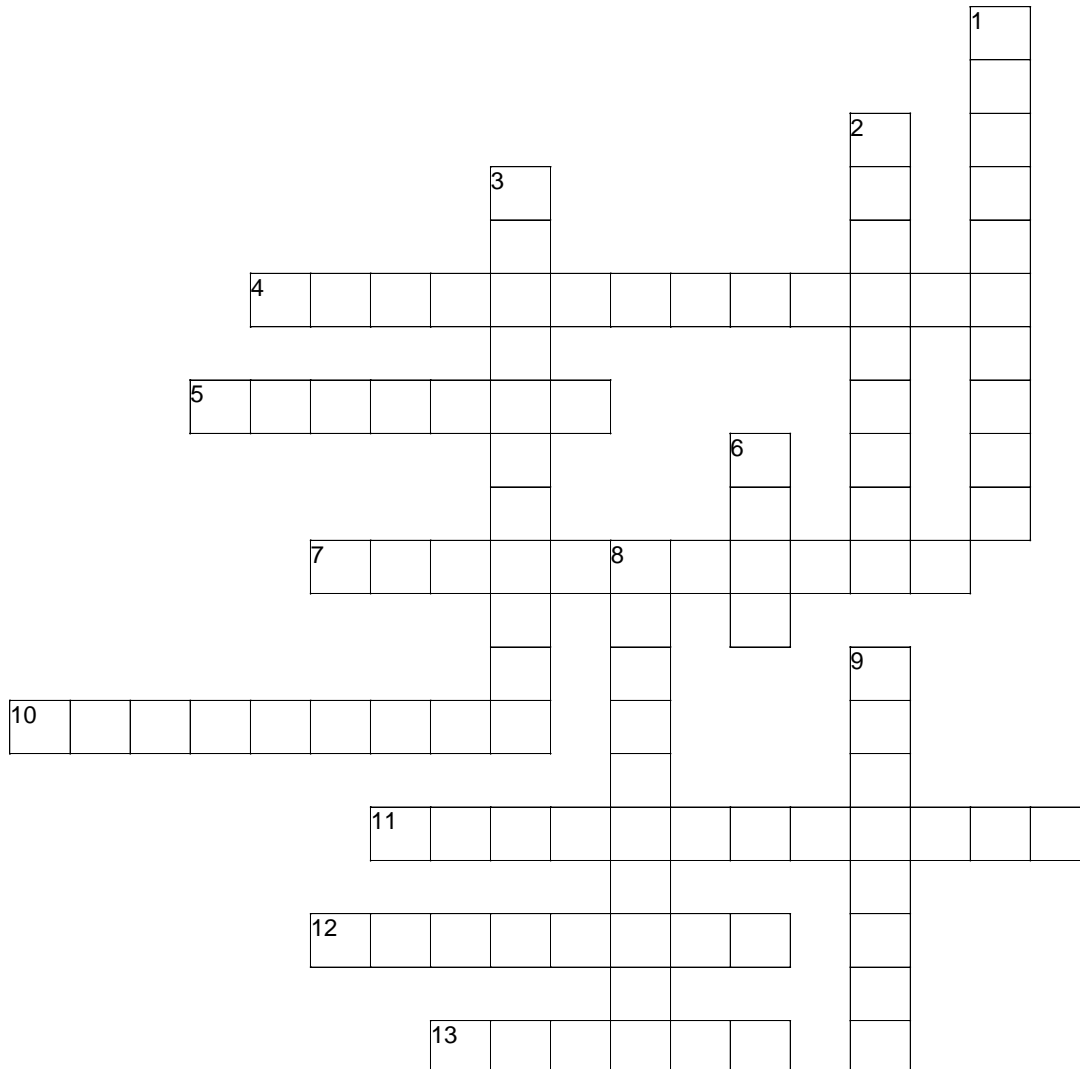
Wire transfer fraud

Identity theft

Spoofing

Tax-related identity theft

Online Awareness CW



Across

4. Report _____ right away.
 5. Check a company's _____ policy before buying.
 7. A scam that requests payment to claim a fictitious lottery or prize.
 10. If you are ever asked to submit this as payment online, it is a scam.
 11. Emails pretending to be from a well-known source asking consumers to enter personal information.
 12. Keep your virus _____ up to date.
 13. Sharing _____ online can make you vulnerable to scammers.

Down

1. The best form of payment to use online.
 2. Fraudsters use the internet and _____ to find victims
 3. Think before you open email _____.
 6. Online general merchandise sales online was the worst _____ of 2020.
 8. A _____ scam involves a romantic relationship online.
 9. Choose a complex _____ for accounts online.

Online Terms Word Find

U X S U T G S M A C S E C N A M O R S D V Z M B
C S U M C F N E R A W T F O S S U R I V I T N A
A M Z K A D E I R P N J Z Z U L M S Q Y F S R C
A A N A S V U H Y S M P Y Y K Y C G M P K E M F
P C I N P V V X T L C M C T W A M F D E K C A H
S S Y L A E E E Y Y L A C K M G N I F O O P S W
M S D E M N G E T C T U A S N I C C O I T W S H
E E E O Y M O R W P A I B E S P F N H U D X O A
M K N X J O C A L A M V T R Z L J C P E P A E D
S A U Y O R M W B S M W I N E N D Y V X N J A J
H T W T U F S L S S G A K R E B X R O C N V X S
S S R U W S S A V W I I R X P D Y C P K B M O O
T P P B G G D M I O C L T G V W I C O F U W O O
N E I L Q R T S C R B P C C A H F F R K F P V X
E E I H R Z A G O D E V W Q H T Z G V C R B U W
M W J L C L H U J S O N L I N E S H O P P I N G
H S U W X X C H D Z F F X D H C S N L E T V I R
C U Z D S O P N L F Y G D N R A R I I J F N M B
A H O S S T A E R H T D F P B S H W P B O D F G
T J Y U U V N P H I S H I N G H H B N L J F N U
T M N Z Z E S E J I Q C C G J A Y S C H Q G H T
A U X Y V G W Z T T O D U Y E P K W C A M N Q R
P T C G F L P J Y Q C J Q F L P Y S H I D F H G
X J M H E S R E T S O P M I V T I H Z F L E O F

Romance Scams Spam Online Shopping Snapchat Instagram
Hacked Malware Cyberbullying Threats Cash App Venmo
Sweepstakes Scams Scams Passwords Antivirus Software
Privacy Imposters Spoofing Identity Theft Attachments
Phishing




Can you recognize a Phishing Email?

Phishing Scams are when fraudsters send emails to potential victims that appear to be from reputable companies in order to obtain personal information such as passwords and credit card numbers.

Only one of the following emails is legitimate, the rest are all phishing attempts. First, can you recognize which email is legitimate, and secondly, can you find at least 2 reasons why each of the other emails are phishing attempts?

#1

 Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
[Amazon.com](#)
Email ID:

#2

NETFLIX

We recently failed to validate your payment information we hold on record for your account. Therefore we need a brief validation process in order to verify your billing and payment details.

www.netflix.com/verification

Failure to complete this validation process will result in a suspension of your netflix membership.

This process will take a couple of minutes and will allow us to maintain our high standard of account security.

Netflix Support Team

This message was mailed automatically by Netflix during routine security checks. We are not completely satisfied with your account information and required you to update your account to continue using our services uninterrupted.

From: account-alert@prime.support <mailaqqos-rm18kcdqouf@romeqemalas.com>
Sent: 18 October 2020 17:06
To: no-reqlv.14769320@web.aqqosupport.com <no-reqlv.14769320@web.aqqosupport.com>
Subject: Reminders: [Latest News Announcement] [Statement of Meeting Agreement] Informed Update - New Notification [#91849441] [FWD]

#3



Thu 9/12/2019 12:20 PM
Office 365 Message Center <support-verification@security-acc.microsoft.com>
Update Your Microsoft Account info Now



Office 365 Microsoft

We are unable to verify Your account Microsoft office information on file for your registration

As a result, your account will not renew and will suspended if you'd like to renew your account please fill out the [Account Verification Form](#) at least 48 hours from now , if you don't verify your account , your account will be suspended.

#4



NETFLIX

New sign-in to Netflix

Hi Karmon,

We noticed a new sign-in with your Netflix account (karmon.snare@gmail.com).

Device

Smart TV

Location

Minnesota, United States

(may not match your exact location)

Time

January 14th, 4:14 PM PST

If you signed-in recently, relax and enjoy watching! But if you don't recognize this sign-in, we recommend that you [change your password](#) immediately to secure your account.

We're here to help if you need it. Visit the [Help Center](#) for more info or [contact us](#).

–Your friends at Netflix

[VIEW ALL TV SHOWS & MOVIES](#)

Questions? Visit the [Help Center](#)

100 Winchester Circle, Los Gatos, CA 95032, U.S.A.

[Communication Settings](#) | [Terms of Use](#) | [Privacy](#) | [Help Center](#)

This message was mailed to karmon.snare@gmail.com by Netflix as part of your Netflix membership.

SRC: 12853_en_US

#5

amazon



**Your Amazon Account are on hold
due to a billing issue**

[Update Payment Information](#)

Due to a problem with your card, we have been unable to charge your payment.

If you don't update your card information in the next 24 hours, your Amazon account are on hold permanently. To continue using your account, please [visit this link](#) to log in to your account and update your payment information.

Thank you,

Amazon.com Customer Service

#6

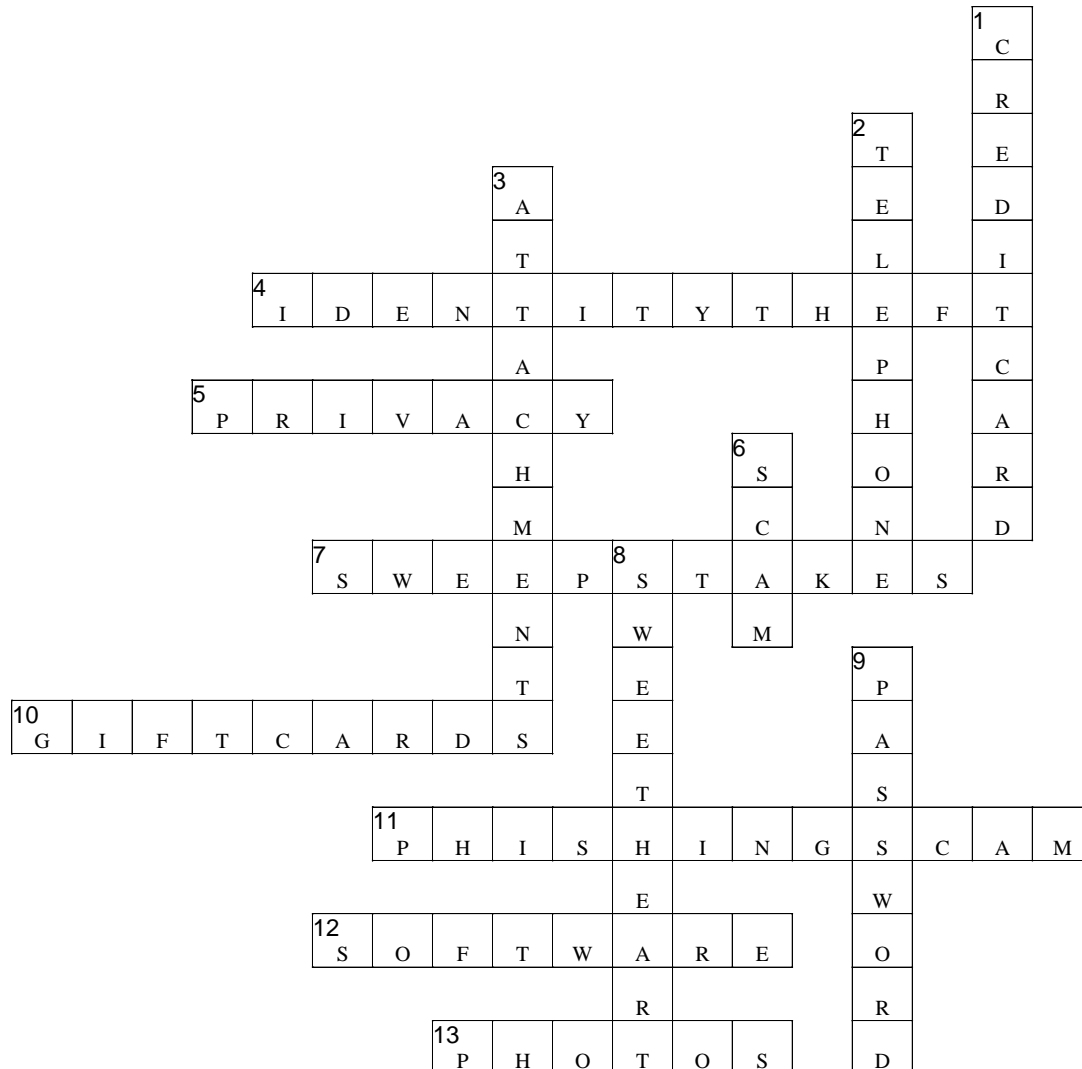
3/12/21 10:48 AM

Venmo Notification : Your account is about to be charged \$192. please review this transaction at <http://transaction-venmo.com/>

Fraud and Identity Theft Scenarios KEY

1. You receive an email that encourages you to click a link and enter personal information, including your Social Security number and bank account number. The email looks official, but the sender's email address seems odd. **Phishing scam**
2. You contact the IRS to ask for more time to file your taxes, but you find out that someone has already filed a tax return in your name. **Tax-related identity theft**
3. You receive a letter from an unknown company with a message that you've won a cash prize. To claim your prize, you'll need to send them your bank account information so they can deposit the money into your account. The company then uses your bank account information to take money from you. **Mail fraud scam**
4. Your caller ID shows that a local number associated with the high school in your town is calling you. You answer and the person calling says they're raising money for a local sports tournament. You soon realize the caller is not actually with the school. **Spoofing**
5. You get a call from someone raising money for a charity. They ask you to wire money immediately because they have a critical and urgent humanitarian need. They get annoyed when you ask them for more information. **Wire transfer fraud**
6. You get a call from someone claiming to be with the sheriff's office. They say they need your personal information to update their neighborhood records. You quickly recognize they're an imposter and not actually who they claim to be. **Imposter scam**
7. Someone pretending to be you used your name and personal information to borrow money to purchase a car. **Identity theft**
8. Your grandmother has a neighbor who has gained her trust but has been secretly taking money from her bank account. **Elder financial exploitation**
9. A hacker stole information from your credit card company, including your personal data, and used it to charge purchases. **Data breach**
10. You receive a letter saying that your house is in foreclosure and will be taken by the bank unless you mail a check and your personal information immediately. You know you've been paying your mortgage on time. **Foreclosure relief scam**

Online Awareness CW KEY



Across

4. Report _____ right away.
5. Check a company's _____ policy before buying.
7. A scam that requests payment to claim a fictitious lottery or prize.
10. If you are ever asked to submit this as payment online, it is a scam.
11. Emails pretending to be from a well-known source asking consumers to enter personal information.
12. Keep your virus _____ up to date.
13. Sharing _____ online can make you vulnerable to scammers.

Down

1. The best form of payment to use online.
2. Fraudsters use the internet and _____ to find victims
3. Think before you open email _____.
6. Online general merchandise sales online was the worst _____ of 2020.
8. A _____ scam involves a romantic relationship online.
9. Choose a complex _____ for accounts online.

Phishing Email KEY

#1 Phishing email



Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

[Amazon.com](#)

Email ID: [REDACTED]

Phishing email indicators:

- Grammar issues, extra spaces between words
- Did you notice you were double charged?
- When you hover over the link, site will not be Amazon
- Why would they suddenly lose your billing address?

What should you do? Go to your Amazon account and verify your information on file.

#2 Phishing email

NETFLIX

We recently failed to validate your payment information we hold on record for your account. Therefore we need a brief validation process in order to verify your billing and payment details.

www.netflix.com/verification

Failure to complete this validation process will result in a suspension of your netflix membership.

This process will take a couple of minutes
and will allow us to maintain our high standard of account security.

Netflix Support Team

This message was mailed automatically by Netflix during routine security checks. We are not completely satisfied with your account information and required you to update your account to continue using our services uninterrupted.

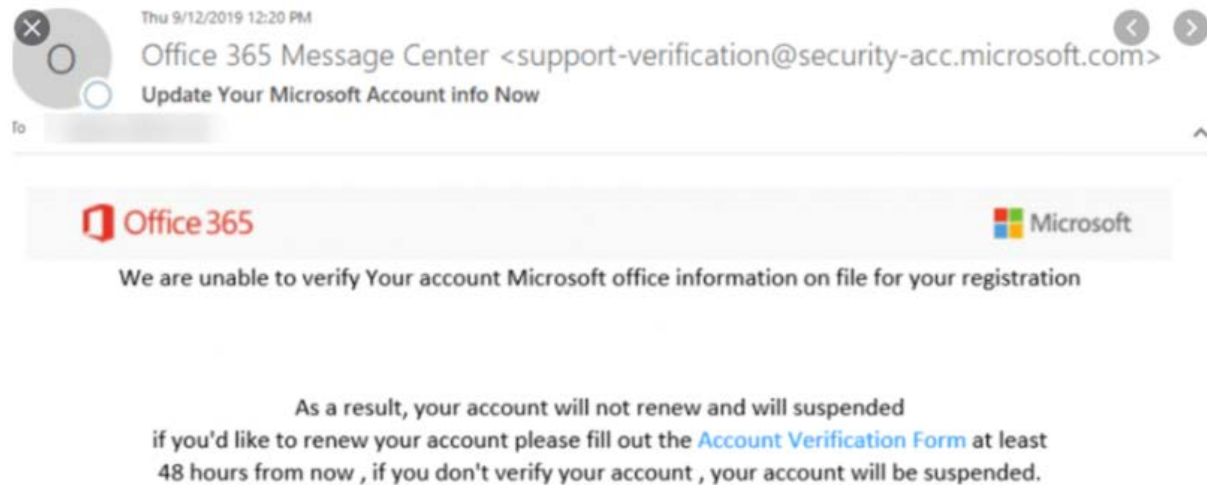
From: account-alert@prime.support <mailqqs-rm18kcdqouf@romeqemalas.com>
Sent: 18 October 2020 17:06
To: no-reqlv.14769320@web.aqqsuqport.com <no-reqlv.14769320@web.aqqsuqport.com>
Subject: Reminders: [Latest News Announcement] [Statement of Meeting Agreement] Informed Update - New Notification [#91849441] [FWD]

Phishing email indicators:

- When you hover over the link, site will not be Netflix
- Threats of cancelling or suspending account
- Grammar issues, extra spaces between words or sentences
- Why would your payment suddenly fail?
- Look at return email address at the bottom (from @prime.support?)

What should you do? Go to your Netflix account and verify your information on file.

#3 Phishing email



Phishing email indicators:

- When you hover over the link, site will not be Office 365
- Threats of cancelling or suspending account
- Grammar issues, extra spaces between words or sentences.
- Why would your account information suddenly be removed?

What should you do? Go to your Office 365 account and see if there are any notifications you need to address.

#4 Legitimate email



NETFLIX

New sign-in to Netflix

Hi Karmon,

We noticed a new sign-in with your Netflix account
([@gmail.com](#)).

Device

Smart TV

Location

Minnesota, United States

(may not match your exact location)

Time

January 14th, 4:14 PM PST

If you signed-in recently, relax and enjoy watching!
But if you don't recognize this sign-in, we
recommend that you [change your password](#)
immediately to secure your account.

We're here to help if you need it. Visit the [Help
Center](#) for more info or [contact us](#).

—Your friends at Netflix

[VIEW ALL TV SHOWS & MOVIES](#)

Questions? Visit the [Help Center](#)

100 Winchester Circle, Los Gatos, CA 95032, U.S.A.

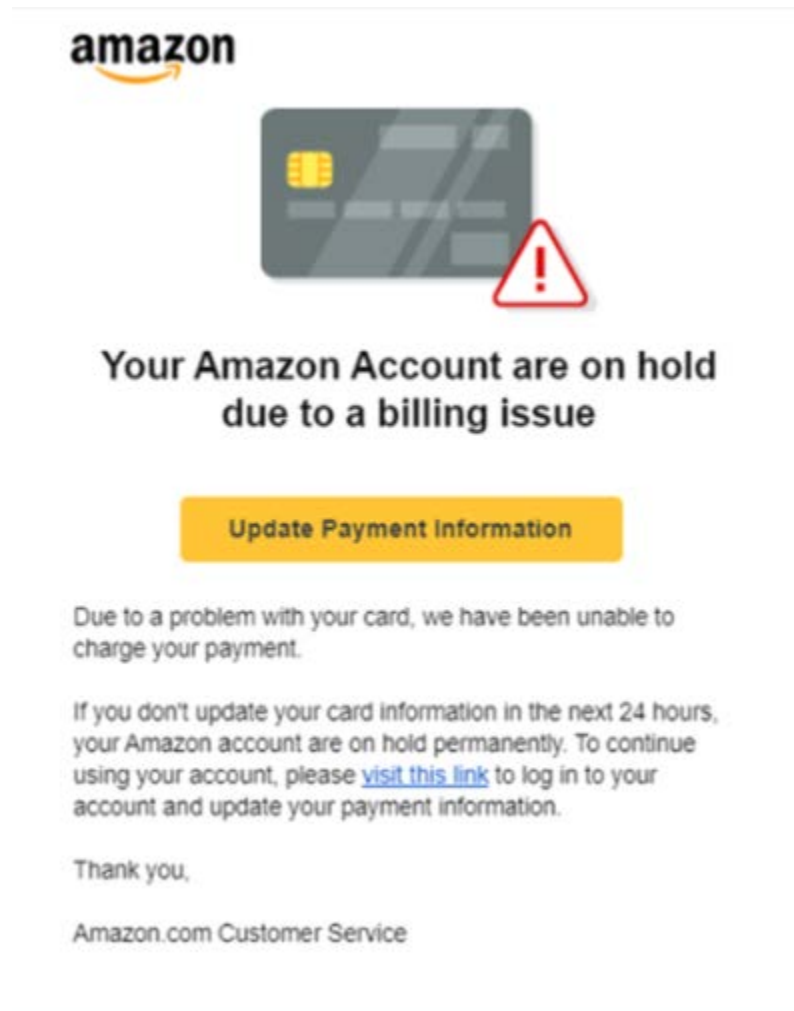
[Communication Settings](#) | [Terms of Use](#) | [Privacy](#) | [Help Center](#)

This message was mailed to [\[karmon_snares@gmail.com\]](#) by Netflix as
part of your Netflix membership.

SRC: 12853_en_US

- You should know if you recently signed-in from a different device

#5 Phishing email

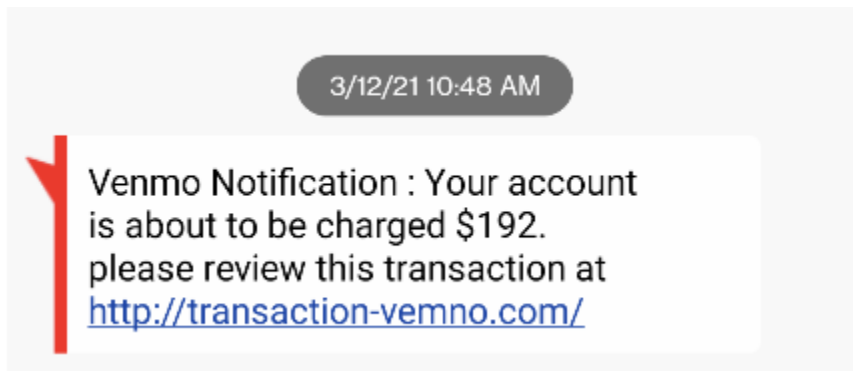


Phishing email indicators:

- Grammar issues, “Your Amazon account are on hold”?
- Threats of cancelling or suspending account
- When you hover over the link, site will not be Amazon
- Why would your card information suddenly be invalid?

What should you do? Go to your Amazon account and see if there are any payment issues.

#6 Phishing Text



Phishing text indicators:

- Very general statement, person asking for payment not named.
- It is usually a large amount (to alert you to act!)
- When you hover over the link, site will not be Venmo
- On the actual link, they misspell Venmo as “vemno.com”.

What should you do? Go to your Venmo account and see if there are any transactions pending.