


The Danger in Disguise:

Social Media, Email, Etc ...



VISHING Overpayment Scams Fake Check Scam Pharming

TICKET SCAMS Cybercrime FEE FRAUD PHISHING

Ransomware Gift Scams **SPEAR PHISHING**

Charity Fra **ROMANCE SCAMS**

SOCIAL MEDIA (FB, TICTOC) Identity Theft

Email Fraud **Scams**

Imposter Scams Technical Support Scams **Door-to-Door Scams**

Pension Scams SMS Phishing

What Do All These Mean ?

How Do They Work ?

Scams can come in many different guises. So it's important to know the warning signs to look out for and what to do if you have, or think that you have been targeted.

Scam Types

Protect Yourself From Scams

<https://www.moneyhelper.org.uk/en/money-troubles/scams/types-of-scam>

<https://www.fca.org.uk/consumers/protect-yourself-scams>

Real Life Examples

Email on Yahoo Mail - looks to be from Google:

Subject: Fwd: Form shared with you: "which our team is currently working on"

From: "Pauline Embry (via Google Forms)" <drive-shares-dm-noreply@google.com>

Date: 9 October 2023 at 12:11:21 GMT-5

To: brenthcooke@ymail.com

Cc: josefermandovega@hotmail.com

kitzya53@gmail.com, sterlingmit

Subject: Form shared with you

Reply-To: Pauline Embry <PaulineEmbry@gmail.com>

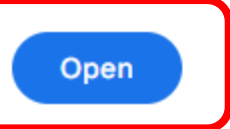
Pauline Embry shared a form



Pauline Embry (PaulineEmbryerxdnqlax@gmail.com) has invited you to **view** the following form:

We are pleased to announce that your online form process has been finished. Go to form

which our team is currently working on



Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
You have received this email because PaulineEmbryerxdnqlax@gmail.com shared a file or folder located in Google Drive with you.

Google™

If you don't want to receive files from this person, **block the sender from Drive**



Real Life Examples

Email on Gmail Acct - looks to be from Amazon
Subject: Your Subscription Has Expired

<http://above.photst.com/fr=6hiOObn6ix3x/%7COxbDn-hK%7ChtPn%7C/NDjnbstXh6i3kRcPC6Dn219LGs9NIK0%7CA6D/n%7CDB2BOjOnkRuXkRfMn%7C%7C6OK>

Welcome Brenthcooke, Your Subscription Has Expired! renew_now 8A... [Box](#)

Prime <support@above.photst.com>
to me

<support@above.photst.com>

Hi

Your PRIME Membership has expired!

prime

[Extend for Free](#)

Dear customer,
Your membership has expired.
But, as part of our loyalty program, you can now extend for 90 days for free. Enjoy free 2-day shipping, Popular movies and hit tv-shows - all available with your Prime membership

[Extend for Free](#)

*After signing up, you have to insert your credit card details for validation of your account. We will not withdraw any amount.

To stop these please go [here](#) or write to:
616 Corporate Way Ste.2-9092
Valley Cottage, NY 10989

Real Life Examples

Email on Gmail Acct - looks to be from Apple about Security
Subject: A recovery contract has been added to your account.

A recovery contact has been added to your account. Inbox x

Apple <noreply@apple.com>
to me

Wed, Oct 4, 9:28 AM (13 days ago) ☆ ↶ ⋮



Did not ask me to CLICK ON anything. They Gave me directions to sign onto to my acct Independently (not through a lick).

A recovery contact has been added to your account.

Dear Brent Cooke,

A recovery contact was added to your account on October 4, 2023 at 10:28:40 AM MDT.

Recovery contacts can help you regain access to your account when you forget your password or device passcode.

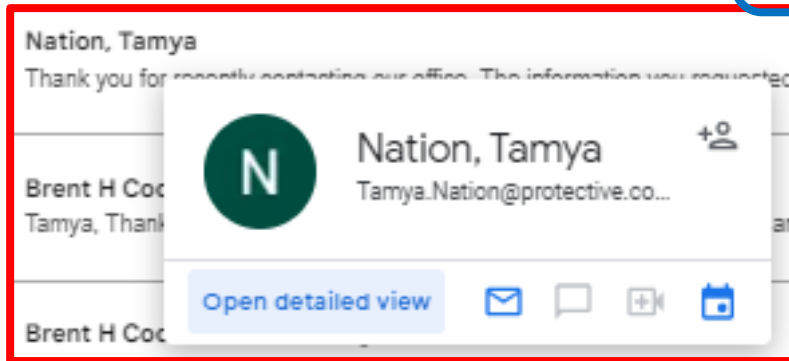
If you didn't add anyone, review and remove any unauthorized recovery contacts from your account as soon as you can. To manage your recovery contacts, go to Password & Security > Account Recovery on your iOS or macOS device.

Apple Support

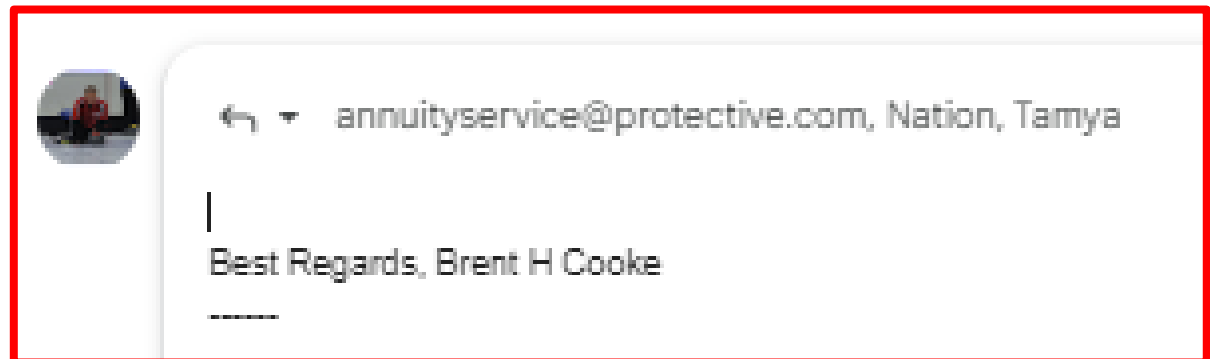
Real Life Examples

Email on Gmail Acct - looks to be something legal (?)

Subject: W-9 FORM.

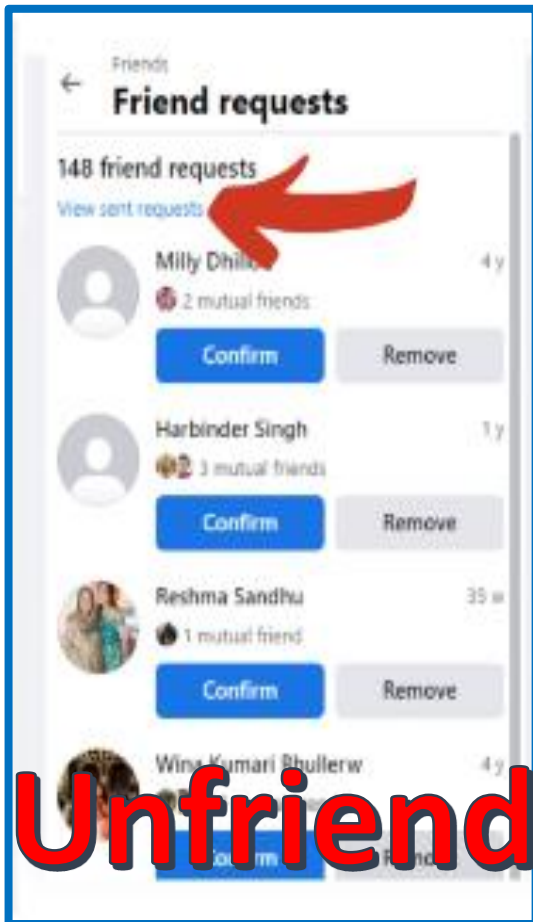


Reply ->



Real Life Examples

Facebook Friend Request - Oh WOW !!!! I havent spoken to xxxxxx in quite a while

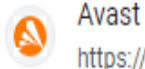


Before You Click “Confirm”

- Is there a picture that you can look at?
- Select the picture and look at the profile. Does it look legit? Hometown? History?
- Look at the pictures in the profile – valid?
- When was the account created? Within 2 months – 2 years?
- Consider calling or emailing them to ask if they sent the request.
- Aren't I already friends with xxxxxx? (check your list)

After You Click “Confirm”

- Do not give out personal information.
- Ask maybe how they are doing along with some random incorrect question:
 - Sorry to hear about MAX – he was a great dog – are you planning to get another?
 - Or a fictitious spouse: Gosh, I haven't seen you and Dianne for like 4 years now – how's she doing?
 - They will either avoid the question or respond suspiciously.



<https://support.avast.com> › en-us › article › antivirus-p...

Why is Avast showing up in my email?

If you use an email client (such as Microsoft Outlook or Mozilla Thunderbird), Avast Antivirus may include a Virus-free message (previously an email signature) at the bottom of your outgoing emails to let your recipients know that the email has been scanned for malware. This setting is enabled by default.

What is the fake Avast warning?

What is the “Avast Your PC Is Infected With 5 Viruses” pop-up? The “Avast Your PC Is Infected With 5 Viruses” alert is a browser-based scam that tries to trick you into thinking that a Avast scan has detected viruses on your device and you need to renew your antivirus subscription to remove them. Feb 19, 2023

- So even when you believe you’re protected, the scammers are still trying to trick you into doubting, and then taking action.
- “Always” go back to your approved source (bank app, web site, device app) to check. “Never” use a link that someone has sent you.

Real Life Examples

Other Scams here in the PHX area – just this year.

Bank Funds Scam: Bank employee called to tell her that her savings acct had been hacked into and \$\$s removed via a fraudulent charge. Helped her through moving the remaining \$\$s to a “temporary holding acct”. 24 hr hold till the account was accessible again.

Result: All \$\$s went missing and no recourse to retrieve as the “temp” acct was fictitious.

Should Have Done: ???

Grandparent Late Night Call: Grandchild called. Person said “Gramma”? Grandparent said a name, and it just went from there. Caller had them hooked and kept them on the phone to xfer funds. Middle of the night – they weren’t thinking straight.

Result: Large sum of money lost .

Should Have Done: ???

Land Title Scam: Fraudsters are submitting “change of ownership” forms for land and residences at the titles office.

Callers Can Reproduce “ANY” Phone Number: If you have numbers in your contact list (your bank, etc) typically 8xx numbers. Scammers will use these. So even though your contact list says “Wells Fargo Support” (contact list) It does not necessarily mean it really is them.

Should Do ???

Spot The Warning Signs

Scams can be **(WILL BE)** difficult to spot. Fraudsters can be convincing and knowledgeable, with websites and materials that look identical to the real thing.

If you've been contacted unexpectedly, or are suspicious about a call or text message, make sure you stop and check the warnings signs.

- **Is it unexpected?** Scammers often call out of the blue. They may also try and contact you via email, text, post, social media, or even in person.
- **Do you feel pressured to act quickly?** Scammers might offer you a bonus or discount if you invest quickly, or they may say the opportunity is only available for a short time.
- **Does the offer sound too good to be true?** Fraudsters often promise tempting rewards, such as high returns on an investment.
- **Is the offer exclusively for you?** Scammers might claim that you've been specially chosen for an investment opportunity, and it should be kept a secret.
- **Are they trying to flatter you?** Scammers often try to build a friendship with you to put you at ease.
- **Are you feeling worried or excited?** Fraudsters may try to influence your emotions to get you to act.
- **Are they speaking with authority?** Scammers might claim that they're authorized and often appear knowledgeable about financial products.

If you answered 'yes' to any of these questions, or you're unsure if a contact is genuine, follow the steps to protect yourself.

How To Protect Yourself

Do:

- Treat all unexpected calls, emails and text messages with caution. Don't assume they're genuine, even if the person knows some basic information about you.
- Hang up on calls and ignore messages if you feel pressured to act quickly. A genuine bank or business won't mind waiting if you want time to think .
- Check your bank account and credit card statements regularly.
- Consider getting independent financial advice or guidance before a big financial decision.
- Check overseas regulators if you're dealing with an overseas firm.
- Install Virus Protection on your computer devices.
- Keep your electronic devices fully updated (OS updates, Virus Protection).

Don't:

- Give out your bank account or credit card details unless you're certain who you're dealing with.
- Share your passwords with anyone (including your social media passwords).
- Give access to your device by downloading software or an app from a source you don't trust. Scammers may be able to take control of your device and access your bank account.

YOU are the first line of defense in protecting your assets



Stay Informed

Phishing Threats in 2023

<https://it.ucsf.edu/new-phishing-threats>

Phishing Threats (by state) in 2023

<https://www.forbes.com/advisor/business/phishing-statistics/>

**Social Media Phishing – The 2023
Cybersecurity Threat**

<https://www.infosecurity-magazine.com/next-gen-infosec/social-media-phishing-threat/>

YOU are the first line of defense in protecting your assets

