

PNYA Scams Targeting Freelancers Notes

Topline advice

- If it feels off, slow down, ask questions. Trust your gut.
- Scams often involve an element of time pressure, don't let that override your suspicions.
- Use two factor authentication and/or passkeys for important accounts, and whenever possible use unique passwords at least 14 characters long.

Common Scams

- Cheque cashing scams - you are sent a check or wire transfer and asked to purchase something or pay someone with the money. The check will later bounce or the transfer will be reversed.
- Fake party invites - may redirect to a fake login page to steal your email login
- Phishing emails from hacked accounts in your contacts

Red Flags to look out for

- Being asked to log into an account you never logged out of
- Emails supposedly coming from a known company, but the email address doesn't match that company.
- Anyone asking you to pay or buy anything for them early on in a job.
- Asking for free "test" work during the interview process.
- Deferred compensation - only agree if the project is worth doing even if you never receive the deferred compensation

What to do if you suspect a scam/have been scammed

- If you suspect a spoofed company or well known person - Look up the company and contact through publicly listed info or ask around your network to get direct contact info.
- If a job seems shady or just poorly organized - get a full contract - can use freelancer's union contract template (see link section below)
- If you have not been paid for a job, you can threaten to go to small claims court, which does not require you to have a lawyer. You can follow through if necessary, but the process is slow.

Useful Resources

Check how likely a site is to be malicious: <https://www.virustotal.com/gui/home/url>

Guide to Passkeys:

https://www.linkedin.com/posts/dariobigi_to-my-applemacios-users-passwords-passkeys-activity-7318332724690255872-FEjb?utm_source=share&utm_medium=member_desktop&rcm=ACoAAABsH1YB1PJvY5v2yczoQakKSF_GaUBQJZ0

Tips for spotting fraudulent recruiters on linked in:

<https://www.linkedin.com/pulse/fraudulent-recruiters-linkedin-dario-bigi-4by8e/>

Check if your email has been in any data breaches:

<https://haveibeenpwned.com/>

Freelancers union - a free to join organization that provides a variety of resources for freelancer including a legal clinic with templates for contracts and demand letters:

<https://freelancersunion.org/legal-clinic/>

<https://freelancersunion.org/contract/>

Article on how to avoid being taken advantage of on Freelance platforms:

<https://blog.freelancersunion.org/2026/07/21/freelance-platforms-is-it-working-the-way-you-want/>

Freelance Isn't Free Act guarantees timely payment for freelance workers. Here is where to file a complaint:

<https://dol.ny.gov/freelance-isnt-free-act>

SPAM EMAIL

SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

FAKE

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!



Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

<http://account.liive.com/ResetPassword.aspx>

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity



Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo*****@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

[Review recent activity](#)

Thanks,
The Microsoft Team

IS THIS A SCAM?

Use this 60-second flowchart before you click



WHEN IN DOUBT: DON'T CLICK. REPORT IT.

Quick stats: 91% of cyberattacks start with phishing • Urgency triggers ~70% of clicks • 2FA blocks 99% of takeovers