

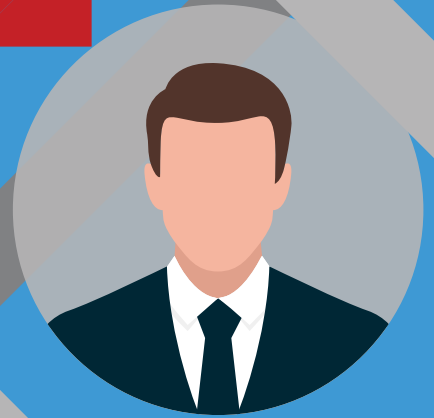


ClearanceJobs®

MITRE

TOP SECRET SOCIAL NETWORKING

**5 TIPS FOR SAFER SOCIAL
NETWORKING FOR SECURITY
CLEARANCE HOLDERS**



INTRODUCTION: Social Networking

Social networking has become ubiquitous in our interconnected, web-driven world. While you used to think of social networking as platforms (Facebook, Twitter, YouTube), social networking can be used for everything from crowdsourcing questions (Quora and Reddit) to finding Fido (Petfinder). If you watched the Netflix documentary the *Social Dilemma*, you may have been tempted to delete all of your social media accounts (but if the film's producers are right, you probably didn't).

Even if you're an active security clearance holder, you don't need to delete every social networking platform. But you do need to be safe. Both active security clearance holders and the defense industry recruiters trying to source them for positions need to be aware of some basic aspects of cyber hygiene.

It's a problem the National Counterintelligence and Security Center (NCSC) knows well, and it is the heart of a campaign kicked off this month in conjunction with the FBI. *The Nevernight Connection* is a new movie released by NCSC and the FBI which details how nefarious actors and foreign intelligence services are using fake profiles and an "invitation to connect" to target national security professionals.

"Social media deception continues to be a popular technique for foreign intelligence services and other hostile actors to glean valuable information from unsuspecting Americans," said NCSC Director William Evanina. "Through this movie and other resources, we hope to raise awareness among Americans so they can guard against online approaches from unknown parties that could put them, their organization and national security at risk."



“Social media deception continues to be a popular technique for foreign intelligence services and other hostile actors to glean valuable information from unsuspecting Americans.”

William Evanina

Director, United States National Counterintelligence and Security Center

COVID-19 and Online Attacks

The coronavirus swept across the country and put thousands of individuals into a remote work environment, often with merely a few days of notice. Government agencies worked quickly to deploy secure remote work options, but hostile intelligence services also worked overtime to attack those newly remote workers as well as systems now operating with limited on-site staff.

“COVID-19 has undermined the cybersecurity of U.S. agencies. Telework and a [400% increase](#) in attacks have allowed for intrusions. Telework places a strain on IT and security resources and these skeleton crews have lost both visibility and the capacity to harden these remote systems,” said Tom Kellermann, head of cybersecurity strategy for VMWare.

The Cybersecurity and Infrastructure Security Agency (CISA) recently released analysis of a cyber attack on a federal agency network. The report is meant as a warning to other federal agencies about what can happen. Using compromised credentials, the cyber actor used malware to gain access using a virtual private network vulnerability the agency knew about. The foreign entity—possibly a major nation state—exploited the agency’s weak firewall to view emails and documents, search for passwords, and basically overrun the system now at its disposal. The CISA report outlines the threat actor activity, and it advises other agencies on protocols to prevent similar attacks. The report shows that just sending employees home with a VPN doesn’t mean data is

protected. And it’s the user (whose stolen credentials opened up access) who remains the most critical point of vulnerability.

Safe social networking applies to both agencies and individuals. A single vulnerable user can compromise an entire network. [Misuse of IT systems](#) is part of the adjudicative criteria—in order to obtain and keep a security clearance, individuals need to demonstrate their ability to comply with IT rules and regulations. In 2015, the then Chief Information Officer at the Department of Homeland Security warned that while misuse of IT systems generally hinges on willingness to compromise information, negligence should be considered as egregious:

“Someone who fails every single phishing campaign in the world should not be holding a TS/SCI with the federal government,” said Paul Beckman. “You have clearly demonstrated that you are not responsible enough to responsibly handle that information.”

Just as candidates have an obligation to keep sensitive information safe, so do companies. The Defense Counterintelligence and Security Agency’s Critical Technology Protection (CTP) mission helps the more than 10,000 companies with facility security clearances safeguard information, technology, and materials. Companies who fail to keep that critical information secure and follow proper protocols could lose their clearances and ability to do business with the federal government.

“I would say that [all businesses regardless of size are vulnerable to the theft of their information](#) regardless of type. Its National Cybersecurity Awareness Month, and that is where all good security begins and ends,” said Matthew Roche, Assistant Deputy Director Operations, Industrial Security Directorate, Defense Counterintelligence and Security Agency. “There are lots of tools out there to help in this regard; seek them out and be obsessive about keeping your devices patched and software up to date.”

With so much at stake—and so much to lose—making sure companies and individuals are staying safe through the primary access point for foreign

adversaries today is ever-important. Here are five tips for safer social networking—they could save your network, and your clearance.

1 'THINK BEFORE YOU LINK'

The UK Centre for the Protection of Critical Infrastructure has a '[Think Before You Link](#)' campaign that mirrors the NCSC and FBI *The Nevernight Connection* campaign. The entire campaign points to the prevalence of social networking attacks originating on LinkedIn. The queries often begin with flattery and pulling information about the individual sourced through public facing online networks and profiles. Sometimes the individual purports to be with a fake company or claims to be a recruiter with a recognizable defense contractor. Fake profiles are prevalent because of how easy they are to set up. And as soon as a fake profile is identified, there are new profiles out there to take its place.

For both the federal government and commercial companies, there is a demand for systems to

identify misinformation and disinformation online. MITRE Social Integrity™ Platform is a hosted ecosystem that provides disinformation and misinformation threat detection.

“One use of our platform is to identify topics that are propagated by inauthentic accounts,” says Mike Fulk, technical lead for the MITRE Social Integrity Platform. “These include algorithm-based, or ‘bot’ accounts, as well as individuals masquerading as someone other than themselves, or ‘sock puppets.’”

As long as there are social networking platforms, there will be individuals using those platforms for nefarious purposes. That’s why the UK is urging its national security workforce to ‘think before you link.’



FOR EMPLOYERS: If you’re pursuing a ‘cold connection’ with a candidate, provide your bonafides up front—including a link to your company website where your identity can be verified.

FOR CANDIDATES: Don’t connect with individuals you haven’t met before. If a ‘recruiter’ approaches you online, it’s okay to ask them to verify that they are who they say they are. Just because you have shared connections doesn’t mean it’s a safe connection.

2 KEEP YOUR PUBLIC FACING PROFILES CLEAN

The reason search engines are so powerful is that they are constantly crawling public facing websites—including social media sites—and aggregating that information. Your LinkedIn, Facebook, Twitter, YouTube, and other social networking profiles are all providing various amounts of information that is searchable. Consider eliminating company names and use extreme caution when listing program titles on

public facing social networking sites. Foreign intelligence agents are experts at connecting the dots between what you list on your profile—and you may be leaving the crumb that leads them directly to a detail they need. Focus your social networking profiles on sharing news updates and information that reveals your personality—not your portfolio of classified projects.

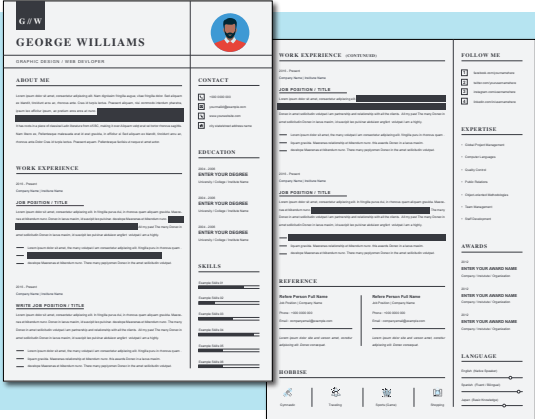


WARNING

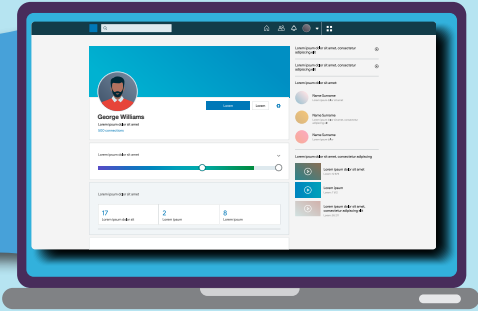
The website ICWatch can best be described as a privacy and national security disaster. It's MO? Cull LinkedIn and Google to create a database of professionals with access to America's secrets. The website boasts that it has gathered more than 400,000 profiles. Everything you post on LinkedIn that links you to the intelligence community could be linking you to third party sites dedicated to 'watching the watchers.'

FOR EMPLOYERS: In today's candidate market, think of your public facing career profiles like creating a dating profile. It doesn't pay to look desperate; it's better to look interesting. If your profile reeks of 'Calling all TS/SCI Clearances,' candidates may think it's China, and not a real recruiter calling.

FOR CANDIDATES: Think about what really needs to live on a public facing profile and what doesn't. Your resume shouldn't be copied and pasted into your LinkedIn or Facebook profile. You can keep your career options open and your information safe.



Redact Sensitive Resume Information Before Posting Online!

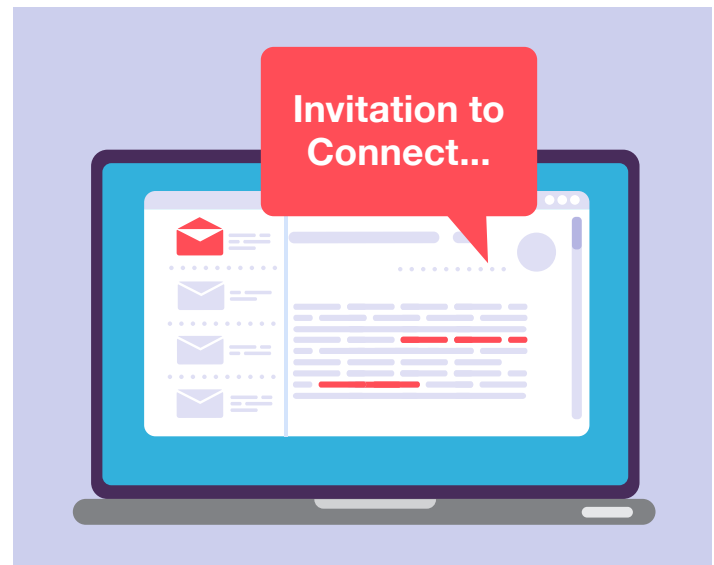


3 BEWARE YOUR EMAIL

Email isn't considered social media, but playing it safe on social networks also involves watching your inbox. According to security awareness research site [KnowBe4](#), LinkedIn tops the list of emails used in successful phishing attacks, with more than half of all social-media related phishing emails originating with LinkedIn.

"This trend has been increasing quarter over quarter, likely because there is a perception that they would be legitimate coming from a professional network," the company reported. "It's a significant problem because many LinkedIn users have their accounts tied to their corporate email addresses."

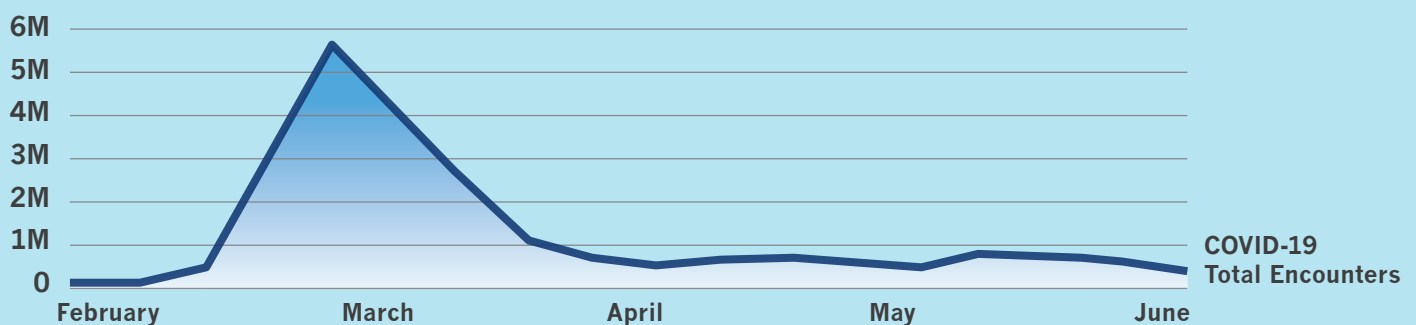
Attacks on networks often originate with compromising a power user, and phishing attacks are a primary mechanism for duping professionals into clicking something malicious and turning over their company or agency's crown jewels. Working



remotely and the slam of COVID-19 news coverage only adds opportunity for malicious attacks.

Microsoft's recently released *Digital Defense Report* noted a spike in malware attacks in March thanks to COVID-19-themed phishing attacks.

Cybersecurity Threat Trends



Source: Microsoft Digital Defense Report

FOR EMPLOYERS: Make your emails to candidates personal. Note how or where you found their profile and an individual detail or piece of information. You don't want your emails to look like a phishing attack.

FOR CANDIDATES: Know that phishing attacks are cyclical and adjust to reflect current news.

4 PRACTICE GOOD HYGIENE

Thousands of new remote workers can open up a Pandora's Box of cybersecurity risks, as cleared professionals suddenly have access to sites they never could have visited on the high side. But just because you have more freedom of access to visit social networking sites from your company computer, doesn't mean you should.

The occasional Facebook check-in is probably fine. But while the lines between work and personal are blended, it's important to remember that if you're working on a government or contractor-provided network, rules of privacy don't apply.

Company rules of propriety, Hatch Act considerations, and security policies all apply

when visiting social media sites from a workplace device. Individuals have lost their security clearances for failing to adhere to company IT policies.

"These cases have almost always involved the viewing of pornographic material on a government or company-owned computer in violation of their employers' rules," said William Henderson, president of the Federal Clearance Assistance Service (FEDCAS). "Most of the other cases also involved workplace misconduct such as: sending inappropriate email, unauthorized viewing of other peoples' email, intentionally deleting files from a server, and preventing access to computer programs."

Continuous Vetting and Social Media

Security Executive Agent Directive 5 issued in 2016 opened the doors for social media information to be used as a part of the background investigation or Continuous Vetting process. But as of today, social media is not a component of making a security clearance determination. Public facing sites, including social media, may in some way be pulled into the government's continuous vetting program. But for now, you don't need to worry about your Facebook posts being used against you in a security clearance denial.



FOR EMPLOYERS AND CANDIDATES: If work and home are bleeding together a bit too much, it may be time to create a line of demarcation. Maybe workplace devices don't go into the bedroom, or agency-issued computers are used only for work, not for social networking. If you're found to be visiting sites you shouldn't during workplace hours or with a workplace device, laziness or negligence claims are not a good defense.

5 REPORT SUSPICIOUS CONNECTION REQUESTS

If you reported every suspect LinkedIn request to your security officer, you'd be sending daily submissions. It's not necessary to report every single request or query, but if something strikes you as particularly sophisticated, or you start to see a pattern in requests you receive, it's certainly worth sending your security officer a notice. If someone strange tries to connect with you and you see they've already connected with a number of individuals with your company, it may be worth checking in with your coworkers to see if the contact is legit. If you ever receive a request from

an individual online that makes you nervous, you can ignore or delete the connection. If a current connection reaches out to you, be cautious. Most malicious requests don't begin with a request to meet for coffee or a free trip to China. They typically involve flattery. That's why it's important to be cautious about what you share. Just because someone expresses interest in your work, seems to have shared work history, and even has shared work connections, doesn't mean they're someone who you should interact with.

Things you can do to keep your profile safe:

- **Lock down your profile**—make your contacts visible to you only.
- **Don't share your phone number, your email list, or your birthday with LinkedIn**—or especially with your contacts.
- **Don't connect to people you don't know.**
- **Never connect/disconnect with the LIONS** (LinkedIn Open Networkers)—they may be real—but their profiles are open and will expose your information.
- **Disconnect from the frauds**—you're lending them credibility even if they can no longer see your contact list.
- **Report frauds to LinkedIn**—it only takes a few clicks!

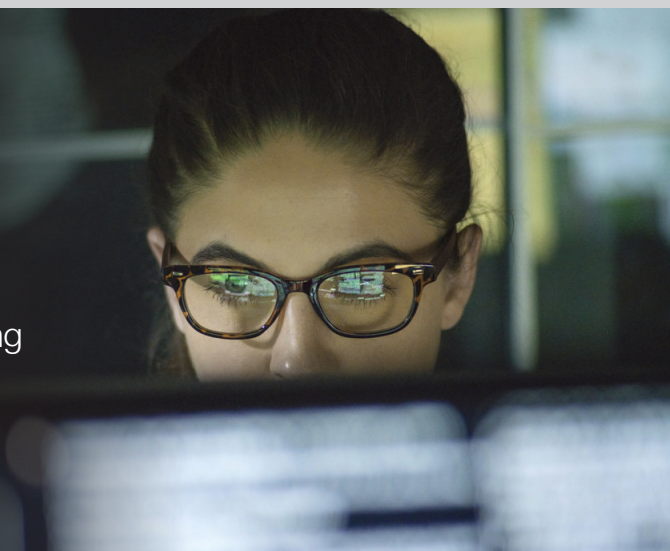


FOR EMPLOYERS: It may be tempting to connect with any candidate with a clearance and a pulse—but candidates can sniff those kinds of connections from a mile away. Carefully cull and vet the connections you make online. Ideally, use social media to reinforce a connection you make via a trusted source like ClearanceJobs.com or a candidate who connects with your company.

FOR CANDIDATES: It goes without saying: don't accept every connection request and report suspicious activity and connections. If a current connection—even a former coworker or trusted colleague—starts to ask for information they shouldn't need or makes you an offer that's too good to be true, consider reporting the activity to your security officer or local FBI office.

COMBATING DISINFORMATION AND MISINFORMATION

There's a plague of disinformation and misinformation infecting our information sources and social media exchanges today. And it's having profound and wide-ranging effects—from undermining the legitimacy of elections to influencing our personal healthcare decisions.

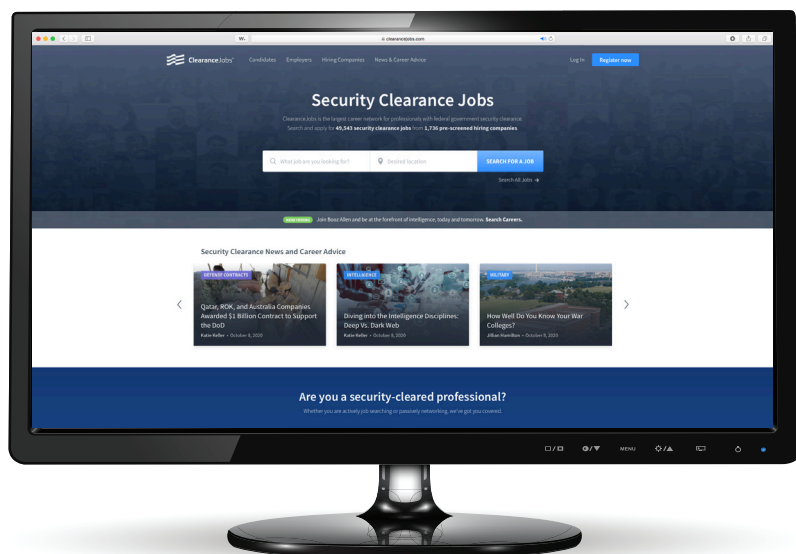


“No single organization can keep up with the scale of dis/misinformation, so we have to come up with creative ways to address it,” says Jennifer Mathieu, chief technologist, social analytics and technology. From MITRE’s perspective, that means mobilizing organizations across the world to work on solutions together.

“Social media platforms are international, so we need to engage globally. We’ve spoken to over 40 organizations in the last two years—including think tanks, nonprofits, fact checkers, academics, industry, and the social media platforms—and everyone agrees with that.”

www.mitre.org/publications/project-stories/combating-social-media-manipulation-globally

© 2020 MITRE



ClearanceJobs is a secure, password protected cleared recruiting marketplace. Authorized defense contractors who register their company with ClearanceJobs must provide the contact information of their company Facility Security Officer. We manually verify the legitimacy of each company and contact their security officer before that company can gain access to our resume database. Unlike other online job platforms, it is not possible to use a credit card to obtain access to the resume database. All employers must go through the manual screening process, and candidate data is not public facing or crawled on the web.

- **PHYSICAL SECURITY**
- **SERVER LEVEL SECURITY**
- **SOFTWARE LEVEL SECURITY**
- **HTTPS TRAFFIC ENCRYPTION**

Learn more about site security on ClearanceJobs.com.