Alliance to Counter Crime Online

'HOW TO' CRIME

Illicit Actors are Training Newbies on Social Media

A research report by

Members

alliance to counter crime online

ABOUT US

The Alliance to Counter Crime Online groups 30 non-profits, academics and citizen investigators collectively fighting the growth of serious organized crime on the surface web. We share a commitment to justice, a dedication to countering exploitation in all its forms, and the courage to investigate some of the worst aspects of humankind. Every ACCO member has taken personal risks and made sacrifices to do what we do, out of passion for the subjects we seek to protect. We need that dedication to take on two of the world's most powerful, well-funded industries: Big Tech and Big Crime. ACCO members are leading authorities in a range of serious crime sectors online, including child sex abuse content, human trafficking, narcotics, wildlife, antiquities, and fraud. ACCO produces investigative reports and analysis about how illicit groups have weaponized social media, and we provide evidence we develop to regulators, lawmakers and the public.

Key Findings

- Organized scammer groups, many of them located in West Africa, use Facebook Groups to share tips about dating, sales, and get-rich-quick scams, which they claim can earn tens of thousands of dollars monthly.

- Far-right extremists use social media videos to offer instruction on everything from personal security to using crypto to move money.

- Purveyors of child sex abuse material (CSAM) share training manuals on the dark web, advising each other on a horrifying range of subjects about how to identify and entrap child victims, and how to store and share CSAM content.

- Wildlife traffickers advertise their services with videos showing how to trap endangered wildlife.

- Animal abusers use 'how to' videos to provide training on dog fighting, or simply to promote their own grisly activities.

- Looters in conflict zones post videos showing how to find buried antiquities using metal detectors and other means. Some offer detailed instructions for what to say to authorities if caught treasure hunting.

alliance to counter crime online

LEARNING HOW TO COMMIT CRIME ONLINE

This comparative study by the Alliance to Counter Online Crime details how illicit networks in multiple serious crime sectors post “how-to” videos on social media platforms, and organize in forums to provide instruction to other would-be law-breakers. In some cases, these criminal trainers even earn money by hosting ads for commercial brands on their instructional videos.

“Organized crime networks aren’t just using social media to predate children, fleece innocent people, and sell them illicit and counterfeit products,” says Gretchen Peters, executive director of ACCO. “They also utilize video platforms, in particular YouTube, Tik Tok, and Facebook, to train and recruit other illicit actors.”

This phenomenon has been in the news recently connected to the so-called Kia Challenge, in which organized crime groups calling themselves the ‘Kia Boyz’ post instructional videos on YouTube and TikTok about bypassing vehicle security, using tools as simple as a USB cable. The Kia Challenge has resulted in thousands of cars being stolen, many of them featuring in social media joyride videos with the perpetrators speeding, swerving, and dangling out of windows.

In May, Kia and Hyundai, the two manufacturers whose cars were most heavily targeted in the challenge, agreed to a $200 million settlement stemming from a class-action lawsuit over ignition security. However, since U.S. law considers user-generated content to represent protected free expression, TikTok and YouTube faced no liability for amplifying this crime or distributing the content.

“How-to” crime videos found during ACCO’s investigation illustrate how to ensnare children for sex abuse, loot cultural heritage sites, conceal far-right extremism, scam innocent, lovelorn people, and trap endangered wildlife.

“Instructional videos and online forums have become a way for offenders to demonstrate how they commit crimes,” says Kathleen Miles, director of analysis at ACCO. "They commonly include tips to help 'Newbies' avoid the attention of authorities and platform moderators."

This investigative report by ACCO, a global network devoted to thwarting international organized crime and exploitation online, is intended to educate the public, governments, and tech companies about a problem that warrants attention.

“We call on social media companies to take a more proactive stance toward rooting out illicit actors exploiting their platforms to train other illicit actors, thus making these problems worse,” says Peters. "And we call on lawmakers around the globe to reform laws that provide a liability shield for hosting this criminal conduct."

Screenshot of SLH's YouTube video.

"Find the perfect target." That is the brazen opening line from a YouTube influencer with 46,000+ subscribers who calls himself "Smart Lazy Hustler" (SLH). In his video series on YouTube, SLH lays out step-by-step instructions for his followers who want to make money by scamming innocent people on social media.

Criminals like SLH are training each other in plain sight on YouTube, one of the world's leading video share platforms, which has removed only one of the dozens of scam training videos reported by ACCO since June 2021. In that same period, SLH's videos alone have more than quadrupled in subscribers and views. His most popular video has more than 296,000 views.

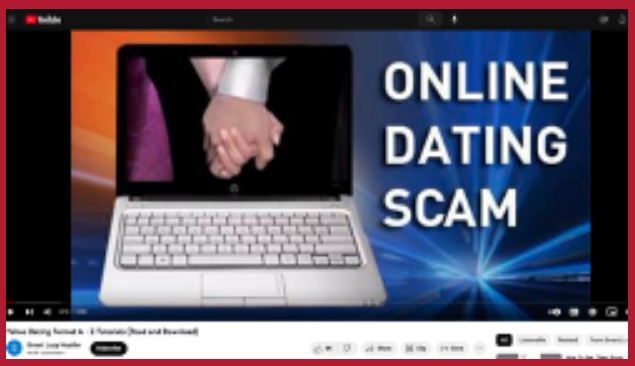
Smart Lazy Hustler is part of a growing trend on platforms like YouTube and TikTok, and online forums where illicit actors organize. SLH does not just use social media to commit illicit activity; he also makes money teaching others to scam innocent people, just like he says he does.

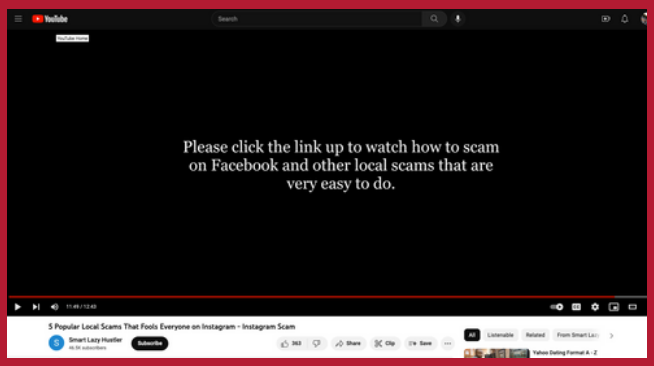
Some scam instructors have become so popular and sophisticated that they even have an AdSense deal with YouTube to make money off commercial brands posted to their videos. For example, when we screened videos for "Mario's Media," a scammer with 26,000 subscribers whose videos feature titles like, "Dating Format for Yahoo Boys," and "How to Get Clients on Facebook," YouTube featured ads for the web design platform WiX and the product analytics platform Amplitude.

Scammers aren't just making money defrauding the innocent. They also profit off training others to become scammers.

alliance to counter crime online

Tech Companies Profit from 'How to' Crime Videos

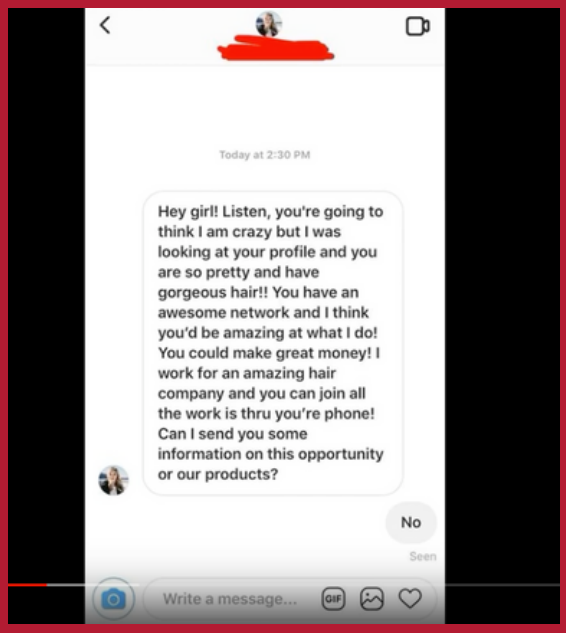




When scammers have advertisements for commercial brands placed on their videos, it means they are technically working in partnership with Alphabet, YouTube and Google's parent company, which shares the ad revenue with creators. In other words, by helping distribute scammer training videos, YouTube becomes an accessory to the crime. Research by Advocating Against Romance Scams (AARS), an ACCO member, found that scammers share these videos in Facebook Groups that serve as educational forums for scammers to trade tips and sell each other images and other identity material stolen from innocent people.

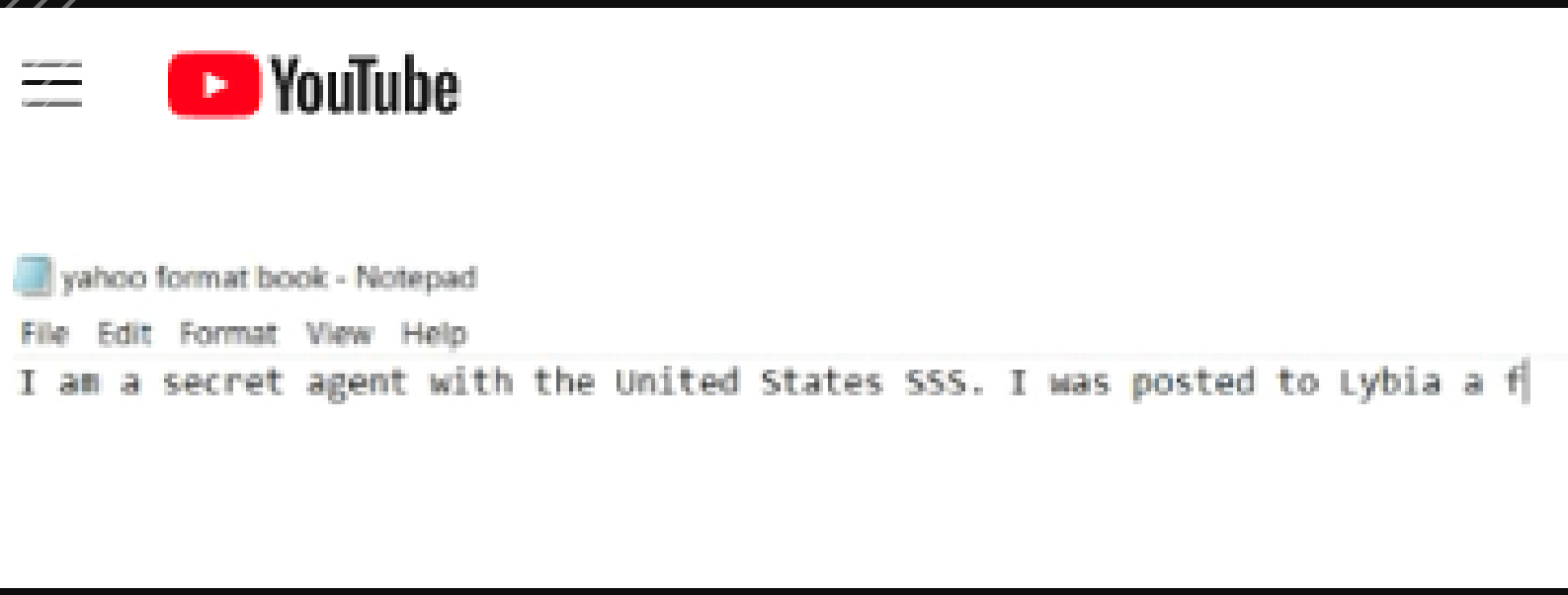
"Virtually every day, we get outreach from a new victim of identity theft or online scamming," says Kathy Waters, cofounder of AARS. "Their stories are often similar, their feeling of loss is very real, and the deceit is debilitating for all involved."

It is hard to imagine how large the scamming community is until you stumble upon it, says Waters, who has spent years penetrating and researching the online forums where scammers train each other. "They have insider terminology and tested methods for getting innocent people to trust them," she says.



Screenshot: Scammer training video.

Visit www.counteringcrime.org to learn how to spot scammers, or follow @AdvocatingforuC on Twitter or TikTok for tips, trends and updates.



A screenshot of Yahoo Boys sharing information on creating backstories for scams.

TARGETING AND EXPLOITING KIND AND LONELY PEOPLE

Scammers know that people looking for love make good marks. "It's very simple. Scroll through dating sites and pretend to be a secret agent," advises SLH. He says your location should be Libya, Somalia, or any place in Africa. Middle-aged women make the best marks, he says. "I suggest you go for women above 45. You might reach out on Plenty Of Fish or like her pictures on Instagram, and once she follows you back, then give her your Gmail."

Then, he suggests, tell the would-be victim you have been a soldier all your life "and try to move the client" to Facebook Messenger or Google Hangouts – but not one associated with your picture or video chat. He counsels his students to check in twice a day, keep notes on what they have told her so they do not contradict themselves, and converse with her for at least three months before they ask for money. Use a VPN to disguise your location and Grammarly to fix your English. When you ask for money, SLH counsels, show the victim how to send money on PayPal, and "avoid Western Union!"

SLH also suggests going after people who are passionate about a pop musician or a political candidate because such people tend to "believe anything." Scrolling through Trump and Biden content on Facebook, he advises, "You will find many clients in the comments section."

Scammers always start by just chatting with their targets. That is because they want to get their targets to reveal their hopes and dreams. “Find their deepest wants,” SLH counsels in a training video, “monitor their mood,” and one day, when they seem happy, ask them for money.

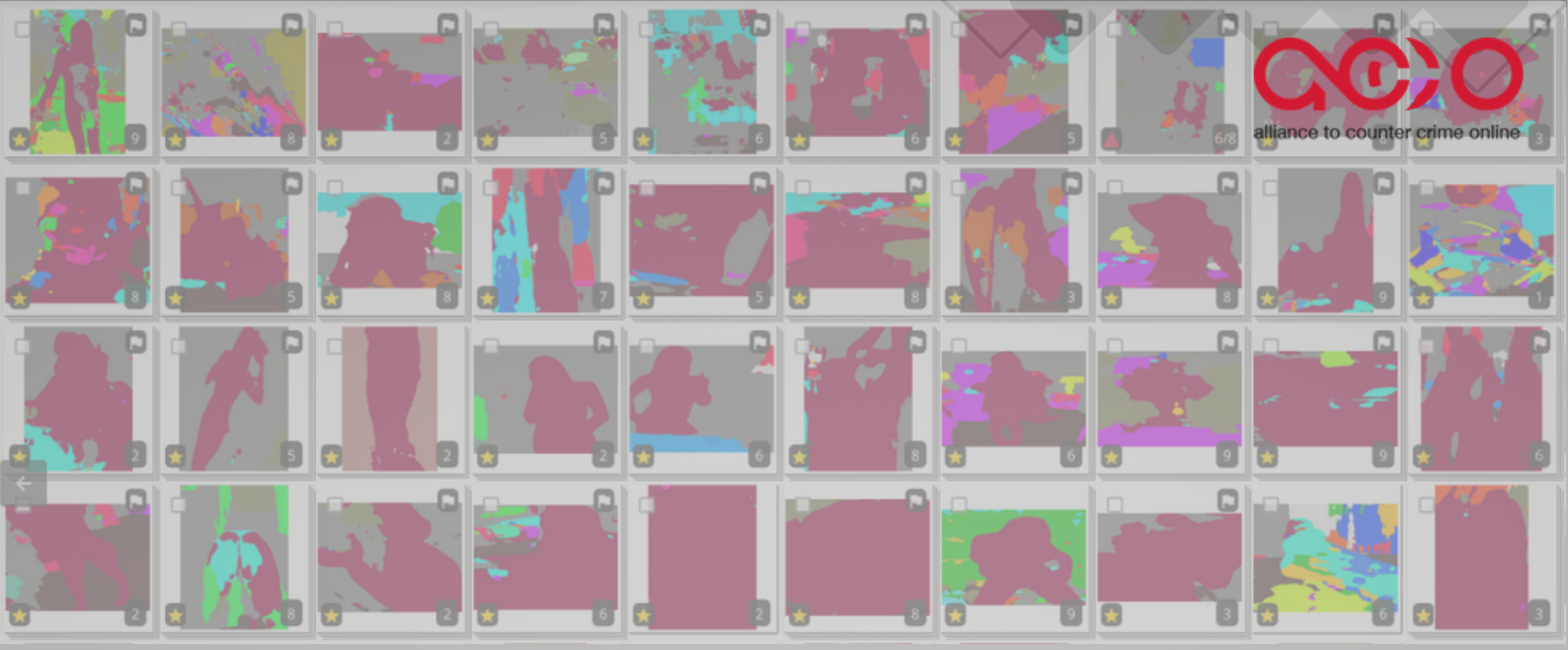
SLH posted another video outlining his favorite scams using Instagram. He calls the first “money flipping,” where you get people to invest, and you give back a bit of money for a while as the pool grows.

But do not try this scam on white foreigners, he warns, because they know what a Ponzi scheme is. “But you can easily target Nigerians who have no idea,” he says. Then there is the charity scam. “I don’t support doing this but if you really need to make money fast, find a picture of someone on the Internet who is suffering, create some Instagram postings, and start marketing it aggressively."

What is his favorite trick? Create a post claiming to sell some popular brand at a discount – he features examples like Yeezy Adidas sneakers and Ray-Ban sunglasses. People will send you money, and you send them nothing in return. To really snare them, he suggests, offer free delivery. "This is a very massive way of making money on Instagram! The trick is not to sell too much to any one client; otherwise, they may come after you."

Another how-to video trains scammers to lure a man to send money by pretending to be a woman. The video on YouTube walks viewers through how they should post a lure using 10 seconds or so of a pornographic video of a woman undressing on a video chat, so the male victim thinks he has a live woman on the other end. The scammer then cuts the video, claiming the Internet signal over Wi-Fi is weak, and asks for money to see more.

Screenshot: Yahoo Boys training video openly available on YouTube.



A screenshot of the Canadian Centre for Child Protection's analyst training software for classifying child sexual abuse imagery.

How Pedophiles Train Each Other in the Dark Corners of Cyberspace

The offending community distributing Child Sex Abuse Material (CSAM) on the open and dark web also runs surprisingly sophisticated training forums. These are primarily hosted on child sexual abuse forums on the dark web, according to the Canadian Center for Child Protection (C3P), an ACCO member that monitors such forums as part of Project Arachnid. In some cases, the forums share PDF training manuals, some as long as 100 pages, that discuss "best practices" for securing and encrypting computer systems to download and share illicit CSAM material, and erasing one's system rapidly, if ever on the verge of getting caught.

These types of instructional manuals also present a horrific menu of topics, ranging from how to identify and target single mothers in ways that will not raise suspicion, to lists of the "best" platforms for finding unsupervised children (spoiler alert: it is social media platforms), and lessons on "capping," a term used by offenders to describe the recording of a child performing sexual acts using a streaming service like Omegle or Twitch.

"What is striking when you read these forums, it is just like they are having a conversation with their buddies over a beer," says C3P's Jacques Marcoux. "Anyone who is not an offender reading these forums would be stunned by the way they casually discuss issues like grooming children and then sextorting them."

The other striking issue is that while the instruction manuals sit on the dark web, the CSAM content is typically stored on the open web. "The anonymity protections of dark web browsers like Tor make it cumbersome to share and download multimedia material," said Marcoux. "So they use the dark web forums to promote and sell passwords and links, and direct offenders to cloud drives where they can download illegal CSAM content."

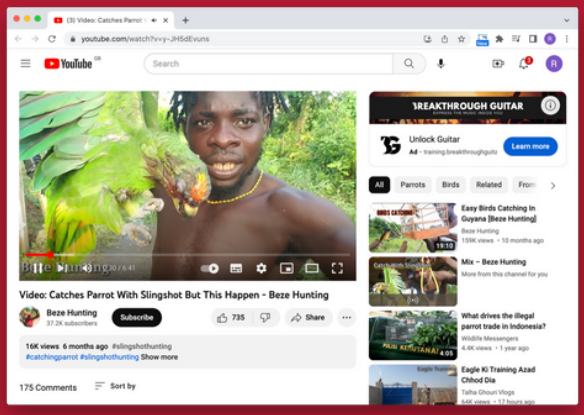
alliance to counter crime online

TRAFFICKERS' GUIDES FOR CATCHING EXOTIC ANIMALS

Among the most colorful ‘how to’ content that experts say is flying below the radar of governments, tech moderators, and even non-governmental organizations that track illicit activities, are “trap gimmick” videos that mimic reality TV shows.

Some of these videos appear aimed at entertaining viewers with creative tricks and gadgets, but principally these videos are intended to teach people how to poach animals or lure in new customers. “Gimmick videos are easy to find and designed as entertainment, apparently aiming to make the subject matter acceptable, and also easy to copy,” says Alisa Davies of the World Parrot Trust, an ACCO member.

Videos show a variety of ways to catch birds including 'mist' nets, painting glue on branches, climbing trees to take chicks from nests, and stunning birds using sling shots. Although sometimes the videos contain messages that they are "for informational use only," the title will explicly say it shows "how to trap owls, parrots and even big cats and other animal species at risk of extinction. In some instances, the makers of the videos will offer the same featured widlife for sale or include their email, Whatsapp number, or Telegram account name in the video."



Video demonstrating how to capture rare, birds and parrots populate YouTube.

Social media use by wildlife traffickers has increased over the past few years, says Davies. While social media companies remove some wildlife trafficking content, they act mostly re-actively rather than proactively, relying almost entirely on activists and conservation groups to alert them to troubling “how-to” videos and other trafficking content.

“YouTube should tighten it's policies on content that involves animals to prohibit content that features the trapping of endangered and protected wildlife.”
~ Rowan Martin, World Parrot Trust

As well as videos showing traditional trapping methods, "gimmick videos" showing animals being trapped using novel trapping methods apparently for entertainment purposes are also routinely posted, according to the World Parrot Trust's Rowan Martin.

“YouTube should tighten it's policies on content that involves animals to prohibit content that features the trapping of endangered and protected wildlife,” Martin said. Animals ensared in these videos also include chimps, apes, reptiles and cats.

Instead, it takes little effort to find videos viewed tens of thousands of times, including one video that has been watched 1.7 million times on YouTube, which claims that using a tree stump trap “works 100%” to capture tiger cubs in Asia.

Some use slick graphics and music, and demonstrate step-by-step instructions for ensnaring exotic animals such as monkeys with bamboo boxes, crocodiles with plastic buckets, birds with soft drink cans, rabbits with cut cardboard, and pangolins with string and PVC pipes. Another common gimmick involves fake “rescue” videos, where they stage a rescue between two animals, or they take a page from wildlife reality TV stars and stage a dangerous climb up a tree to rob parrot nests, ACCO researchers have found.

“Some people call themselves rescuers, but they’re really exploiting animals. Unfortunately, people watch these videos and believe them,” says Nina Jackel of Lady Freethinker, an ACCO member focused on protecting animals from cruelty. In 2021, Jackel’s nonprofit sued YouTube for breach of contract with its consumers for allowing the uploading of animal trapping, dog fighting, and animal abuse videos, and failing to delete them when alerted by activists.

“How-to videos make it easier to get to people. It’s an underappreciated aspect of wildlife trafficking, and under the radar. Animal cruelty gets attention, but not so much the instructional material like this,” Martin says.

A violent sub-sector in the world of online animal abuse are training videos related to dogs. This video, found on Facebook, demonstrates methods for training pitbulls and rottweilers for dog-fighting.

alliance to counter crime online

TREASURE HUNTERS TRAIN ON GEAR, LOCATION, & LYING TO COPS

Another international illicit crime sector known for self-labeling social media posts and instructional videos as “faked for entertainment” is the looting of cultural heritage sites in conflict zones, according to Dr. Samuel Andrew Hardy, an ACCO member, who also supports the Heritage Management Organization.

Dr. Hardy studies the connection between archeological crime, conflict, and political violence. He has often uncovered ties between looters and smugglers who bribe government forces to move items through front lines in conflict zones, or even work directly with members of state and non-state forces profiting from the trafficking of antiquities.

Ukraine is a current example of a conflict zone that has been the victim of military looting since the Kremlin’s invasion of Ukraine in early 2022.

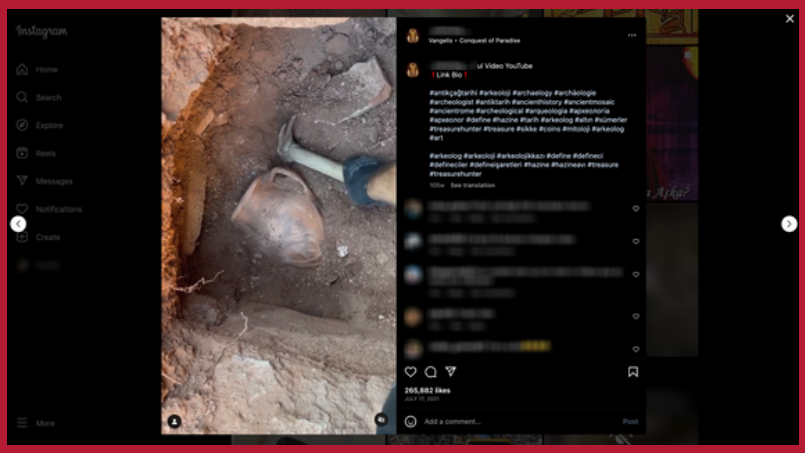


Photo (above) from an illegal dig posted on Instagram.

A post on Facebook (right) explaining how to find hidden artifacts.

“Instagram and Facebook posts teach people what kind of metal detector they need for finding certain antiquities.”
~ Dr. Samuel Hardy, Heritage Management Organization

Dr. Hardy says much of the instructional material on social media describes what gear to use, and how not to get caught by police and other authorities.

“Instagram and Facebook posts teach people what kind of metal detector they need for finding certain antiquities. Or, treasure hunters post memes about the risk of getting blown up by the dynamite they use for illegal excavations,” Dr. Hardy says.

"There are also posts about how to dig up antiquities. Some post advertisements to pitch themselves as brokers or consultants in South and Southeast Asia, offering to help find antiquities in exchange for splitting any profits. And they explain how to devise a cover story for the digs – even if it’s on their own land," he notes.

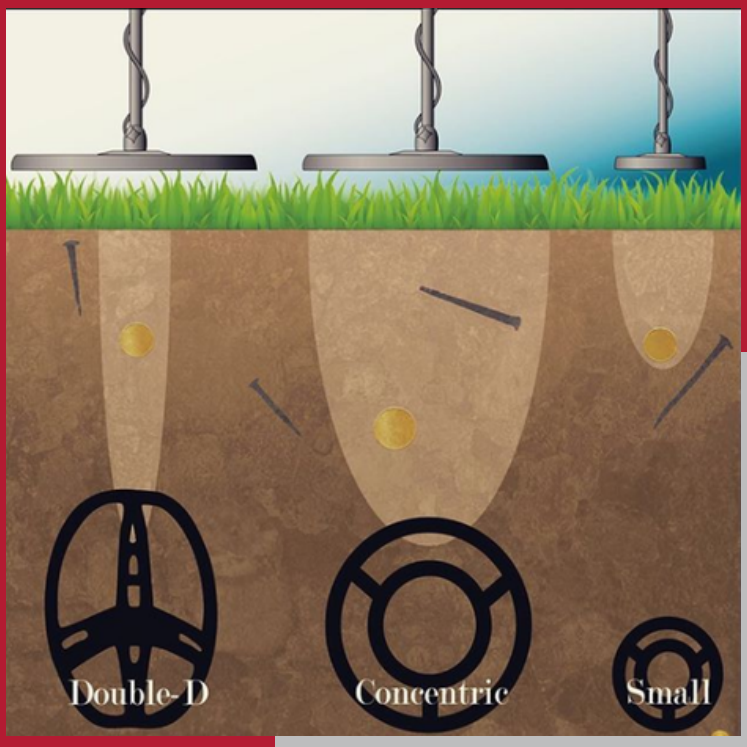
They also suggest creative excuses to provide authorities should they be discovered digging with a metal detector. One video suggests claiming that one is searching for a lost tool, a wedding ring, or buried pipes ahead of construction work.

“They’ll suggest looters tell any curious police, ‘I’m so glad you’re here, officer, I was going to report these things I found while looking for my lost property.’” In the UK, the word used to glamorize this activity is “nighthawking,” with looters calling each other "Nighthawks." One social media influencer who loots ancient sites advertises her own treasure-hunting services on social media. “Much of this is flying under the radar of governments and NGOs. Some haven’t bothered to understand it because there is so little scrutiny of it,” Hardy says.

The problem is especially acute, as the looters well know, in lawless conflict zones from Afghanistan and Colombia to Syria and Yemen.

One brazen antiquities dealer linked to organized crime figures, who is tracked by Hardy’s group in Western Europe, posted a video on Facebook pointing out regions of the world that are beyond any government’s control.

The treasure hunter claims metal detecting and looting is legal in these lawless zones and features a map to advertise where he operates.



A photo posted on Instagram demonstrating types of metal detectors to use.

alliance to counter crime online

EXTREMIST VIDEOS TRAIN ON CRYPTO & SECURITY

Evading law enforcement scrutiny over time became a priority for extremist movements and their affiliated networks. Their online videos – be it Islamist jihadists or Neo-Nazis – have evolved from espousing ideology to teaching followers how to fly under the radar of governments, according to researchers at the Counter Extremism Project (CEP), an ACCO member.

The Islamic State in Iraq and Syria (ISIS) took propaganda to new levels of depravity almost a decade ago, and the group still produces significant output on social media. However, with the destruction of their "caliphate" in the Middle East, ISIS shifted its messaging to instructing its supporters on moving currency and operating undetected.

"While we are not seeing the same levels of how-to content as we did in the past," says CEP Executive Director David Ibsen, now "videos are warnings to look for infiltrators."

"It's almost counter-intelligence or preventive instruction," he adds.

CEP researchers monitor the output of Taliban, al-Qaeda, and ISIS online, and have found that much of their digital content now focuses on how to use cryptocurrencies and peer-to-peer technologies to transfer funds and payments.

ISIS Explosives Manual posted on Google Drive was still available on October 11, 2022, despite it having been reported to Google on August 15, 2018.

> "Videos are warnings to look for infiltrators – it's almost counter-intelligence or preventive instruction."
>
> ~ David Ibsen, Counter Extremism Project

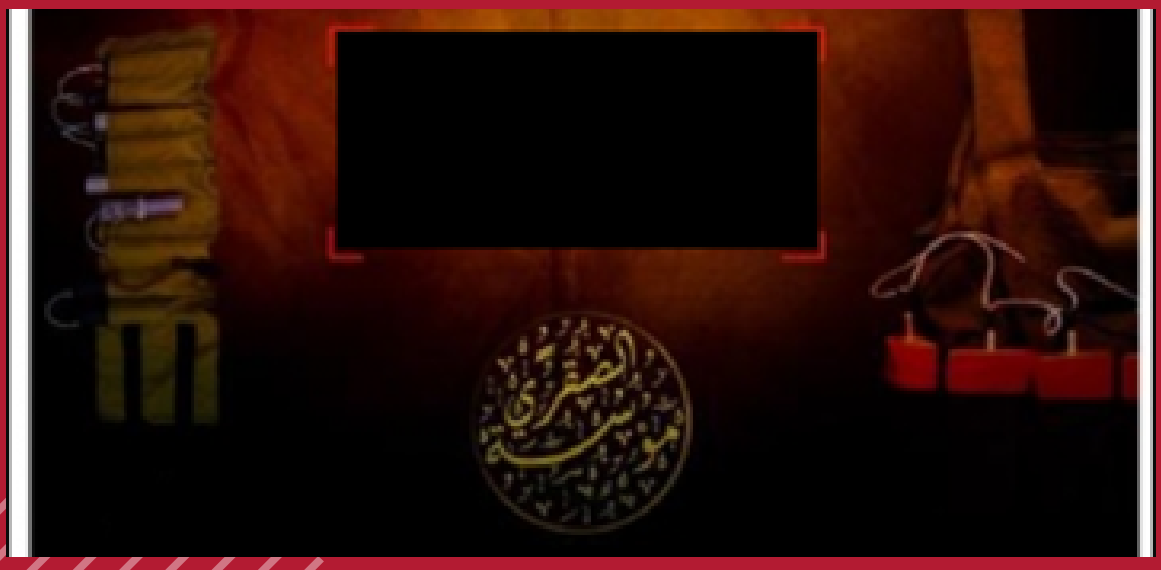
CEP also notes that this type of instruction is now shared among white nationalists and right-wing extremists on both sides of the Atlantic, with a focus on personal security measures, such as keeping track of the most secure encrypted messaging apps.

"Videos we have seen are mostly about technical issues, such as educating fellow extremists about their legal rights after a police raid," says CEP Senior Director Dr. Hans-Jakob Schindler. "There are also videos from extremists and terrorists to their sympathizers online about how to use newer cryptocurrency systems that are nearly impossible to crack and how to conduct good business practices."

There is even some overlap with the trapping and poaching of African wildlife, since many of the regions most affected by militant activity are also home to exotic wildlife that has monetary value, Schindler says.

Another thing both jihadism and far-right extremism have in common with wildlife poaching is the response by major social media companies.

"The global social platforms do little about it even when they are alerted to it," Schindler says.



Al-Saqri manual located on, and since removed from, the Internet Archive.

Conclusion & Recommendations:

ACCO produced this research after realizing in our member meetings that researchers across a range of serious crime sectors were observing the same phenomenon: online training manuals and forums for perpetrators of serious organized crime. We call on authorities and tech platforms to address this under-studied phenomenon, and to focus on removing these online forums, manuals, and training videos, in order to make it harder for illicit actors to learn from each other.

We call for:

- Lawmakers in countries currently preparing legislation to reform how cyberspace is governed should specifically address this phenomenon, creating a duty of care for tech platforms to identify, remove, and report illicit instructional material posted by users and other illegal conduct.

- Policymakers in law enforcement and regulatory agencies tasked with monitoring and restricting illicit activity in cyberspace should add this problem set to their menu of responsibilities.

- Tech companies, in particular, Meta (which owns Facebook and Instagram), ByteDance (which owns Tik Tok), and Google (which owns YouTube), should implement policies to restrict, remove, and report forums and videos where illicit actors train each other on how to exploit innocent people. Tech moderators might also learn from existing videos to develop mechanisms to block illicit and exploitative actors.

- Governments should increase funding for public education programs that educate ordinary people on how to stay safe online.

alliance to counter crime online

We're fighting to make cyberspace safer

Are you worried about getting scammed online?
About endangered species disappearing?
About children being trafficked for sex?
Do you hate what social media has become?

If you support what we are doing, please send a donation. Every gift counts.

DONATE