First Bank & Trust Company

The Bank That Puts You First

Member FDIC

May 2022

The Inexpensive Tools Cybercriminals Use to Steal Your Information

Crooks use a variety of tools and tactics, but smart security practices can thwart them.

Just as any legitimate enterprise today requires tech expertise to keep computers and networks running, so do fraud enterprises. The difference, if you believe the movies, is that the person in charge of tech at a criminal operation would be a young, slightly crazy computer genius, able to type 200 words a minute and penetrate the Pentagon's most secure computers in seconds, simply for fun.

But most cybercriminals aren't tech geniuses. The tech tools of criminality are relatively easy to find, buy and use. Order some computers and headsets, get top-grade internet service, buy and install the right software, teach your workers to use it and other online tools, and your boiler room can be up and running quickly.

Here are some common tools used by cybercriminals:

The dark web

This underground part of the internet began as a project developed by the U.S. Navy to allow intelligence operatives to communicate with each other anonymously. Over time, the Navy made its Tor browser "open source," meaning anyone could use the dark web, including you and me — and for free. That has proven to be a jackpot for criminals. Because of its ability to keep users anonymous, tech specialists train scam artists how to use it to communicate, share information, buy stolen goods and services, and plot criminal activities.

Telegram

That's the name of a secure, encrypted, private messaging app owned by Pavel Durov, a Russian billionaire. Telegram is notoriously unfriendly to law enforcement, and so it has become the new favorite meeting place of online crooks and scammers.

Continued on page 2

Member FDIC

EQUAL HOUSING LENDER

Virginia Bank Locations
Abingdon, Virginia, East
276-628-3838
Abingdon, Virginia, West
276-628-9558
Blacksburg, Virginia -
540-951-1656
Bridgewater, Virginia
540-266-0003
Bristol, Virginia, East
276-466-9222
Bristol, Virginia, West
276-669-1122
Christiansburg, Virginia
540-260-9060
Fairlawn, Virginia
540-633-3793
Hanover, Virginia
804-550-5700
Harrisonburg, Virginia
540-434-0671
Lebanon, Virginia East
276-889-3401
Lebanon, Virginia West
276-889-4622
Lynchburg Virginia
434-455-0888
Norton, Virginia
276-679-7401
Staunton, Virginia
540-885-8000
Verona, Virginia
540-248-7700
Waynesboro, Virginia
540-943-5020
Wise, Virginia
276-328-3439
Woodstock, Virginia
540-459-7228
Wytheville, Virginia
276-228-1125
Operations Center
276-623-2265

Tennessee Bank Locations
Bristol, Tennessee
Volunteer Pkwy
423-652-2022
Gray, Tennessee
423-467-9966
Johnson City Tennessee
423-975-9900
Kingsport, Tennessee
423-246-3700

First Bank & Trust Loan Production Offices
Bedford, Virginia
540-583-5458
Daleville, Virginia
540-966-7006
Hanover, Virginia
804-550-5700
Lynchburg, Virginia
434-509-0444
Mount Airy, North Carolina
743-212-2013
Red Oak, North Carolina
252-220-4208
Roanoke, Virginia
540-774-0269
Rocky Mount, Virginia
540-484-0338
Winchester, Virginia
540-545-8110
Wytheville Annex

First Bank & Trust Mortgage Lending Division
Bristol, Virginia
276 -644-9900

PII — Personal identifiable information
Every form of financial cybercrime has an element of identity theft. It takes sophisticated technology to create a storefront for this info that law enforcement can't easily penetrate. Criminal websites such as Robo-check — which lists the Social Security numbers and dates of birth of millions of Americans — are well known to law enforcement, but they are hard to shut down. But cybercriminals also use many legal websites to obtain public information about you, including AnnualCreditReport.com, Delvepoint, TLO, Intelius and BeenVerified.

Your internet-browsing "fingerprints"
Sophisticated business websites collect dozens of unique attributes about the device you use when you visit. Those characteristics are individual enough to identify you out of potentially millions of other users. Today's criminal tech gurus often try to steal your browser fingerprint. Those fingerprints are then sold to other criminals on the black market for as little as $3 each. That can allow crooks to convince online retailers like Amazon and Walmart that they are logging in with your smartphone.

Burner phones
Sometimes, scammers need to provide a phone number to a business to complete a scam (say, set up a new bank account in your name). While certain digital approaches can work, often a criminal simply uses a physical prepaid cellphone. The cost for one of these burner phones? Around $40.

Spoofing tools
Websites such as Phone-Gangsta and Spoofmycalls enable cybercriminals to spoof various phone numbers on a caller ID. They can appear to be the IRS, law enforcement, your financial institution — or even you. Cost: 10 cents per minute of a phone conversation.

SOCKS5 proxies
This technology allows criminals to hide their physical location online. They might be in Ghana, Nigeria or the U.K., but they can make it look like they're in Florida, California, New York or anywhere else they choose. The cost is about 30 cents for access to the proxy.

Fake driver's licenses and documents
Successful online crime often requires the crook to provide proof of identity or address. So, like in the movies, illegal businesses exist that can deliver on these needs. Counterfeit driver's licenses can sell for $40. Fake documents proving address (billing statement) often sell for $25.

Remote desktop protocols (RDPs)
A hacker gains access and control of a target's computer. He or she can then grant that access to other criminals to use to commit crime. RDPs are used to provide a clean, untraceable connection for criminal use. The cost is typically $5 for each session in which the hacker logs in remotely.

Cryptocurrency expertise
Bitcoin, Monero and Zcash are among the rising number of online currencies used by criminals to launder money, to pay for criminal goods and services, and as a form of payment for ransom. Using them effectively can require tech expertise.

How to protect yourself

- Change the passwords on important accounts (credit cards, banks, frequently used retailers, and so on) every three months. Make them "passphrases" — a random combination of words, plus numbers and symbols, to make them impossible to guess.
- Record your passwords in a highly secure password manager system or write them in a book you hide in your home. Never keep passwords in a list on your computer.
- Take alerts about potential data breaches from online organizations seriously. If you get a message that a breach involving your information has occurred, immediately review your account and change the password.
- Purge your social media accounts of any personal info you wouldn't want a stranger or thief to have. Such information could range from your home or email addresses to photos of vacations and birthday celebrations.

***Source:** Brett Johnson, AASP, April 18, 2022*

Learn a New Survival Skill: Spotting Deepfakes

What Are Deepfakes?

The word "deepfake" is a combination of "deep learning" and "fake." Deepfakes are falsified pictures, videos, or audio recordings. Sometimes the people in them are computer-generated, fake identities that look and sound like they could be real people. Sometimes the people are real, but their images and voices are manipulated into doing and saying things they didn't do or say. For example, a deepfake video could be used to recreate a celebrity or politician saying something they never said. Using these very lifelike fakes, attackers can spin up an alternate reality where you can't always trust your eyes and ears.

Some deepfakes have legitimate purposes, like movies bringing deceased actors back to life to recreate a famous character. But cyber attackers are starting to leverage the potential of deepfakes. They deploy them to fool your senses, so they can steal your money, harass people, manipulate voters or political views, or create fake news. In some cases, they have even created sham companies made up of deepfake employees. You must become even more careful of what you believe when reading news or social media in light of these attacks.

The FBI warns that in the future deepfakes will have "more severe and widespread impact due to the sophistication level of the synthetic media used." Learn to spot the signs of a deepfake to protect yourself from these highly believable simulations. Each form of deepfake — still image, video, and audio — has its own set of flaws that can give it away.

Still Images

The deepfake you may see most often is the phony social media profile picture. Clues in still images are not easy to spot and can be hard to identify:

⇒ ***Background:*** The background is often blurry or crooked, and may have inconsistent lighting such as pronounced shadows pointing in different directions.

⇒ ***Glasses:*** Deepfakes often have mismatching connections with slightly different sizes or shapes.

⇒ ***Eyes:*** Deepfake photos currently used for fake profile pictures appear to have their eyes in the same spot in the frame, resulting in what some call the "deepfake stare."

⇒ ***Jewelry:*** Earrings may be amorphous or strangely attached. Necklaces may be embedded into the skin.

⇒ ***Collars and shoulders:*** Shoulders may be misshapen or unmatching. Collars may be different on each side.

Video

Researchers at the Massachusetts Institute of Technology, MIT, developed a question list to help you figure out if a video is real, noting that deepfakes often can't "fully represent the natural physics" of a scene or lighting.

⇒ ***Cheeks and forehead:*** Does the skin appear too smooth or too wrinkly? Is the age of the skin similar to the age of the hair and eyes?

⇒ ***Eyes and eyebrows:*** Do shadows appear in places that you would expect?

⇒ ***Glasses:*** Is there any glare? Too much glare? Does the angle of the glare change when the person moves?

⇒ ***Facial hair:*** Does the facial hair look real? Deepfakes might add or remove a mustache, sideburns, or beard.

⇒ ***Facial moles:*** Does the mole look real?

⇒ ***Blinking:*** Does the person blink enough or too much?

⇒ ***Lip size and color:*** Do the size and color match the rest of the person's face?

Audio/Voice

Researchers say technologies like spectrograms can show when voice recordings are fake. But most of us do not have the luxury of a voice analyzer when an attacker calls. Listen for a monotone delivery, odd pitch or emotion, and lack of background noise. Voice fakes can be hard to detect. If you receive an odd call from a legitimate organization, you can verify if the call is real by first hanging up then calling the organization back. Be sure to use a trusted phone number, such as a phone number you already have in your contact list, a phone number printed on a bill or statement from the organization, or the phone number on the organization's official website.

Conclusion

Be aware that attackers are actively using deepfakes. They can make fake accounts on social media to connect with or create fake videos to influence public opinion. Some are even selling their services on the dark web so other attackers can do the same. We don't expect you to become a deepfake expert, but if you arm yourself with the basics of identifying the fakes, you'll be far better at defending yourself. If you suspect you have detected a deepfake, report it to the website or source that is hosting the content.

Source: ***Kerry Tomlinson, OUCH! Newsletter, March 1, 2022***