

Don't Make It Easy for Them



Make Life Difficult for Cybercriminals

You don't have to make life easy for cybercriminals – and you don't have to be tech savvy to adopt the behaviors that make their jobs tough. They log off empty-handed, and you can enjoy the internet and all the scrolling, shopping, and clicking you can handle!

We present to you a few **real scammers**. While some of them have been arrested, more are following in their footsteps, and we want you to make their lives difficult.

Here are the punks who are hoping you'll take shortcuts.



Meet dpxaker: Long, unique passwords are too much work for him!

Dariy Pankov, known among hackers as “dpxaker,” paid for his lavish lifestyle by selling password-cracking software to criminals for just \$250 – no subscription required. Powered by his program, hackers don’t have to sit in a dark room guessing passwords one at a time – dpxaker’s software and AI tests thousands of password combinations every second. These hackers love pet names and birthdays – they really love short passwords and reused passwords!

DON'T MAKE LIFE EASY FOR DPXAKER

- Every password should be at least 16 characters long
- Every password needs to be unique to the account
- Every password should be a random mix of letters, numbers, and symbols
- Use a password manager to create and store awesome passwords – they are safe, easy to use, and many are even free!

An 8-character password can be cracked in seconds, no matter how many &s and !s you use. A complex 16-character password takes billions of years to crack – and hackers don’t have that kind of time!

Meet Zestix: MFA is such a pain

Zestix invaded more than 50 multinational companies because a few people never turned on multifactor authentication. And if some of the biggest companies in the world can go down, it would be very easy for Zestix to zestily hijack any of our accounts if we only protect it with a password. After swooping up stolen passwords on the Dark Web, criminals can break into many accounts that don’t enable MFA. They can also get their hands on passwords lost in data breaches and spray them all over the internet with automated software. Unfortunately, it’s easy to nab a password these days... and criminals love it when it’s all they need.

DON'T MAKE LIFE EASY FOR ZESTIX

- Enable multifactor authentication (MFA) on every account that offers it
- Use an authenticator app (Duo, Google Authenticator, and Microsoft Authenticator, for example) or biometrics (like FaceID) whenever possible
- Don’t reuse passwords or iterations (like adding \$ to another password)

Turn on MFA for every account!

Meet Cozy Bear: Roar back with software updates

Cozy Bear, a cybercriminal organization backed by Russia, stays in business by constantly hunting for outdated and unpatched software. Sometimes, the hunt is simple – the moment a company releases a software update, they study it to see what vulnerabilities it fixes. Then they peek around the web for companies and people who haven't installed it yet. In a way, they get a how-to guide for infecting your machine. Every day you click "Remind Me Later" for an update is another day Cozy Bear hopes you're vulnerable... and they want to make your life a lot less cozy.

DON'T MAKE LIFE EASY FOR COZY BEAR

- Turn on automatic updates whenever possible
- Check regularly that operating systems, browsers, apps, and devices are updated
- Restart devices when updates require it

Updates don't just add features. They are full of Bear repellent. Most operating system updates take 5 minutes or less, even including restarting your device. Just do it when prompted, enjoy the little break, and don't make it easy for them!

Meet Giant Company: Don't take their bait

Giant Company was one name for a massive scam operation based in Myanmar but targeting regular Americans like you and your grandma. Almost 300 people were arrested in connection with the Giant Company, and 9 scam centers were disrupted as part of the crackdown. But Giant Company is a drop in an ocean of scams. Scammers and phishing attackers impersonate your bank, your boss, a delivery company, customer support, or even a family member. They want you to click their links, take their phone calls, open their DMs, respond to their "accidental" texts, and, eventually, send them your hard-earned money.

And now with AI, scammers can do more crime every day! These big scamming syndicates love to make you feel something and act fast.

DON'T MAKE LIFE EASY FOR GIANT COMPANY

- Be extremely suspicious of every unexpected inbound message, especially if it seems urgent
- Take a few seconds (4-9 seconds) when reviewing all communication
- Look out for urgency, like fear ("you just got hacked!") and pressure ("you won an expensive grill!")

You don't need to click. You don't need to respond. You don't need to answer the phone. You aren't being rude. Their biggest enemy isn't technology. It's your skepticism.

Make life hard for them

You don't need to know how all the scams work. You don't need expensive tools. You don't need to be an expert. Here's what you should do to Stay Safe Online:

- Every password should be 16 characters long, unique to the account, and a random mix of letters, numbers, and symbols
- Use a password manager to create and store your passwords
- Enable multifactor authentication for every account
- Keep your software updated
- Scrutinize every unexpected inbound message, especially if it seems urgent or requests payment

For more free, fun cybersecurity tips and tricks, check out our Cybersecurity Awareness Month campaign and **sign up** for our free email newsletter.