Scams

CUCUG
Quentin Barnes
December 18, 2025

Scams

- *Everyone* is vulnerable to being scammed
- But like with locks, you want yours good enough to encourage scammers to go try elsewhere
- The way to make yourself less interesting is through education and good practices

Scammers' "Target"

- Father of a family friend
- Lives in town, in his 70s
- Lost a substantial amount of his life savings
  - Unsure what, if any, he'll get back
- This incident is all active and ongoing
  - Second hand too, so some details might be wrong

r/Scams subreddit

- Target got hit by a combination of scams
  - Some I recognized from reading r/Scams regularly
- Knowledge is power
- Consider joining
  - If not, at least read its popular scam summary list

Initial Entry Point

- Target called support at a big, well-known cable ISP
  - After initial problem, asked for additional help with his printer
  - Support said he'd need to make an appt with a "technician"
- Immediately received an (888) call, thought it was a tech
- Caller had him run remote desktop session via browser
  - Caller opened a command line under Windows 11
  - Ran CLI script installing a RAT (Remote Access Trojan)

Good Practices - Phone Calls

- If a caller isn’t in your phone’s Contacts, ignore it!
  - That is, *any call* that shows up on your screen with an area code or a country code
  - If it’s important, they can leave you voicemail
- If a caller *is* in your Contacts, don’t necessarily trust them either
- If you must answer a call, never believe Caller ID or Caller Name
  - Trivial for scammers to spoof caller info
  - If area code is the same as yours, don’t believe caller is local
  - No matter what the person says, never give *any* personal info
  - Scammers are spoofing numbers and in real time faking familiar voices with AI

Good Practices - Phone Texts

- Texts from “short codes” usually are real
  - Numbers with 6 digits or fewer are corporate owned
- Like with calls, ignore any sender not in your Contacts
  - Anything showing an area code or country code, shields up!
  - If sender is in your Contacts, caution is still recommended
- *Never* reply at all to a text unless you know already know the person
  - Even harmless looking ones like “Hey”
  - Leaves you vulnerable to Wrong Number scams
  - Replying validates to the scammer your number is a working number

Good Practices - Contact Info

- Don’t just google contact email or phone numbers
  - Using SEO, scammers can boost their fake sites
- Use the phone number on back of your bank card
- If you have to google, use whois to check domain
  - Scam domains are usually only a few months old at best
  - Check its nameservers too
  - Not foolproof though, scammers can hijack an old domain

Your Phone Number

- Target had his phone number “stolen”
  - SIM swap attacked (ported out)
- Scammers used his phone number to reset passwords
  - Got into his financial accounts
- *Never* use your phone number for any important account as part of its authentication (2FA, password reset/recovery)
- Have your cellular service provider block port-outs
  - Not always a guarantee though, but can help

Your Email

- Target used one email account for everything
- Made scammers job easier
  - Account flooded with worthless emails burying important ones from his financial institutions
- Use different email(s) for financial institutions
  - No spam should show up there either!

Password Hygiene

- Target had used short passwords (8-9 chars)
  - Often not unique or only varied by 1 or 2 chars
  - Wrote passwords in an old address book
- Already gave a talk on this topic in July
- Will be helping Target convert to a pw manager

Credit Bureaus

- Target did get a fraud alert placed on his credit report
  - Fraud alerts are shared among the three
- Target did not understand that fraud alerts do not freeze
  - Fraud alerts do not stop hard pulls
- Freeze your credit reports!
  - Must be done at all three bureaus separately
  - Ignore “locks”, ignore anything wanting to charge you
- Check your credit reports

Brokerage Accounts

- Target got his brokerage account drained
  - Account is at a very well-known brokerage firm
  - Funds were transferred out to another very well-known firm
  - Scammers took advantage of a hole bypassing security
  - Hole is likely still there
- If you have a brokerage account, create “empty” (unfunded) accounts for yourself at all the other major brokerage firms
- Target did not have the apps for his banks and brokers installed with notifications enabled