Cyber Attacks, Online Scams, and You

Paul S. Wang, Sofpower.com

May 19, 2025

In the digital age, our security has two aspects–in the physical space and in cyberspace. Most of us are more familiar with the former but much less with the latter. Yet both are equally important. Of course, it is essential for everyone to become more knowledgeable about cyber attacks and online scams, because they can cause harm, even disaster, to businesses and individuals.

Companies as well as governments must devote resources to protect themselves and people they serve. Individuals also want to be vigilant and avoid becoming victims.

We'll look at cyber attacks and online scams, as well as how to deal with them, in simple and easy to understand terms with particular focus on online scams. Topics here can not only help individuals become better prepared but also enrich their *Computational Thinking* (CT).

This article is part of our ongoing CT blog published in *aroundKent* (`aroundkent.net`), an online magazine. Other cyber security and engaging CT articles can also be found in the author's book *Becoming A Computational Thinker: Success in the Digital Age*. See the website `computize.org/CTer` for more information.

Let's begin with cyber attacks.

Cyber Attacks

In *cyberspace*, where communication over computer networks takes place and where our online accounts and critical private data reside, a lot of great things can happen. But, at the same time, bad things such as various attacks, by

faceless characters from any part of the world, can also happen. Such things include delivering unwanted or unwelcome materials, eavesdropping, breaking and entering, information theft, datanapping, and other cyber crimes. Surely, we want to take full advantage of the web/Internet while guarding against possible downsides.

Widely publicized security breaches range from information theft to influencing democratic elections to holding computers for ransom. No wonder why many individuals feel edgy about their own security and privacy online. You are not alone if you feel unsure or even helpless.

While cybersecurity is a vast area and involves many factors and players—Internet providers, computer software and hardware companies, search engines, social media, and government agencies—here we focus only on a basic understanding of safety measures for individual users.

High-Profile Attacks

Let's first take a look at some high-profile cyberattacks in the recent past.

Cyberattacks

- **Baltimore city public schools data breach (2025)**: The data breach impacted over 31,000 individuals, including employees, volunteers, contractors, and a portion of the student population.
- **Port of Seattle data breach (2024)**: The Port revealed that 90,000 people were impacted after their personal information was compromised by a ransomware attack from the criminal organization known as Rhysida.

- **Colonial Pipeline ransomware attack (2021)**: In May 2021, the Colonial Pipeline, a major fuel pipeline operator in the United States, fell victim to a ransomware attack. The cybercriminal group known as DarkSide was responsible for the attack, leading to the shutdown of the pipeline for several days and causing disruptions in fuel supply across the US East Coast.
- **SolarWinds cyberattack (2020)**: One of the most significant cyber attacks in recent history, it targeted the software company SolarWinds, allowing hackers to infiltrate its systems and gain access to numerous organizations worldwide.
- **WannaCry ransomware attack (2017)**: This attack affected hundreds of thousands of computers worldwide. It exploited a vulnerability in Microsoft Windows systems and spread rapidly, encrypting files and demanding ransom payments in Bitcoin. The attack targeted various organizations, including healthcare institutions and government agencies.

WannaCry Ransomware Attack

- **Equifax data breach (2017)**: In one of the most significant data breaches in history, the credit reporting agency Equifax suffered a cyberattack that exposed personal information of approximately 147 million people.
- **Sony Pictures Entertainment hack (2014)**: The attack leaked sensitive data, internal emails, and unreleased films and was attributed to the hacker group known as Guardians of Peace and was believed to be motivated by geopolitical tensions. The incident resulted in significant financial losses and reputational damage to Sony.
- **Target point-of-sale systems attack (2013)**: Customer credit card data were stolen one day before Thanksgiving 2013.

Who and How

Cybersecurity attacks can be launched by a single individual or a well-organized group. Some, the so-called *advanced persistent threat* groups, could be connected to industry or even governments. Generally, a cybersecurity attack exploits one or more vulnerabilities in a system or network, including the Internet as well as phone networks. Here are some types of attacks that should concern end users.

- Phishing—Collecting private or confidential information such as user IDs, passwords, Social Security numbers, driver's license numbers, account numbers, phone numbers, PINs, addresses, and birthdates by tricking users to supply them through phone calls, emails, or fake websites. For example, an email may ask the user to increase email storage space, verify an online order, confirm a refund or payment, change login information, fix an old unpaid invoice, or manage a package delivery by clicking a link in the email. The link leads to an official-looking online form put up by the attacker. Or, a scam may inform you of a sudden wealth that you can receive by sending your bank account information and often a handling fee or tax! Originally done through email, phishing can now take many approaches such as *smishing* (via SMS) or *vishing* (via voice call or messaging).

A Phishing Attack

- Spoofing—Pretending to be someone, at some IP address, from a certain website, sent from some email address, or located at certain GPS locations. Spoofing is usually done by falsifying data used in communication protocols. For instance, by spoofing the email `From` header a scammer can send an email to you that appears to be from a person you know.

- Malware—Malicious software of all kinds including computer viruses, ransomware, worms (spreading themselves through the network), Trojan horses (hiding in seemingly legit applications), keyloggers, spyware, and rogue security programs.
- Eavesdropping—Spying by secretly monitoring network communications or leaking electronic emissions from equipment. For example, unencrypted messages sent over the Internet are readable by anyone. The man-in-the-middle attack carries this further by intercepting messages between two correspondents, and perhaps even altering the messages as they are passed along to the other end.

Cybersecurity Checklist for Everyday Users

To enhance cybersecurity, let's have a checklist for ordinary users.

General Safety Practices:
Safeguard your user ID and password; use strong, unique passwords for each account (use a password manager); enable *two-factor authentication* (2FA, e.g. login+texting, email, Q&A), wherever possible; keep devices and software updated (OS, browser, apps, antivirus); back up important files regularly (cloud or external drive).

Smart Behavior Habits:
Don't click on suspicious links or attachments in emails or messages; avoid logging into sensitive services (like banks) on public/shared computers; never reuse work passwords for personal sites, and vice versa; log out of accounts after use, especially on shared devices; don't share or lend your phone, tablet, or laptop to others.

At Work or Shared Environments:
Lock your computer when stepping away (e.g., Windows+L, or close lid); avoid entering passwords on someone else's device; don't plug unknown USB drives into your computer; clear browser history, cache, and cookies after using a public workstation.

Mobile Device Hygiene:
Use a PIN, fingerprint, or face unlock on your phone; install apps only from official stores (Google Play, Apple App Store); review app permissions — deny access to things apps don't need; turn off Bluetooth and Wi-Fi when not in use, especially in public places.

Network Usage:
Avoid accessing banking or sensitive info on public Wi-Fi; use a VPN when using public networks, if possible; disable auto-connect to Wi-Fi networks; avoid entering personal information on sites without HTTPS.

Extra Protection for Financial & Critical Accounts:
Use a separate device (or browser) dedicated to banking and sensitive accounts; monitor your bank and credit activity regularly for any strange behavior; use credit over debit for online purchases —better fraud protection.

Privacy and Personal Data:
Limit how much personal info you share online (birthdate, location, etc.); be cautious with social media posts that can hint at passwords (pet names, school names); review privacy settings on your accounts regularly; be skeptical of unknown friend requests and messages.

Scams–Attacks with Victim Participation

While many attacks involve breaking into computer systems, networks, cellphone systems and online accounts without alerting the victims, other attacks known as *online scams* actively involve the victims by tricking them into evil plots designed to steal their money, information, or worse (kidnapping, human trafficking).

Online Scams

Here is our top-ten online scam list.

1. *Job Offer Scams*: Scammers offer fake job positions, often promising high pay with little work, and then try to get victims to pay for training or equipment.

2. *Phishing*: Scammers use fake emails, texts, or social media messages to trick victims into revealing personal information like passwords or financial details.

3. *Imposter Scams*: Scammers impersonate government officials, family members, or legitimate organizations to gain trust and extract money or information.

4. *Romance Scams*: Scammers create fake online profiles to build relationships and eventually ask for money, claiming they're in an emergency situation.

5. *Tech Support Scams*: Scammers call or email pretending to be tech support professionals and trick victims into paying for services or revealing personal information.

6. *Fake Check Scams*: Scammers send fake checks for payments and then instruct victims to send part of the amount back, often in cash, only to later discover the check is fraudulent.

7. *Online Shopping Scams*: Scammers create fake online stores to sell products that are never delivered or are misrepresented.

8. *Investment Scams*: Scammers promise high returns on investments that are often not legitimate, such as Ponzi schemes or pyramid schemes.

9. *Lottery Scams*: Scammers promise to give victims lottery winnings but then require them to pay fees to claim the prize.

10. *AI-Enhanced Scams*: Scammers use AI to create more realistic and convincing scams, including deepfakes, AI-generated images, and fake voices to trick victims.

Pot of Gold

Spotting Scams

The most common tell-tale signs of an online scam include suspicious requests for personal information, urgency and threats, unrealistic offers, requests for unusual payment methods, poorly written communications, unverified websites or social media profiles, scammers who won't meet in person, promises that are too good to be true, requests for payment before shipping, and a lack of detail in their statements.

More details about these tell-tale signs:

- **Requests for Personal Information**: According to the Federal Trade Commission, scammers often ask for sensitive data like Social Security numbers, bank account details, or passwords. Legitimate businesses rarely request this information directly.
- **Urgency and Threats**: Scammers use pressure tactics like "act now" or threatening consequences to manipulate victims.
- **Unrealistic Offers**: Promises of huge prizes, guaranteed returns, or incredibly low prices are often a sign of a scam.
- **Unusual Payment Methods**: Scammers often prefer methods like gift cards, wire transfers, cryptocurrency, or money orders.
- **Poorly Written Communications**: Scams often contain typos, grammatical errors, awkward phrasing, and not addressing you or anyone in particular.
- **Unverified Websites or Social Media Profiles**: Legitimate businesses usually have verified social media accounts and secure websites.

- **No Contact Info**: Scammers don't want you to get back to them, let alone meeting you in person.
- **Promises That Are Too Good to Be True**: Scammers offer unrealistically high returns, prizes, or discounts.
- **Requests for Payment Beforehand**: Scammers usually ask you to prepay various charges such as taxes, handling or shipping fees.
- **Lack of Detail**: Scammers often provide vague or incomplete information, and no actual contact information, unlike legitimate businesses who offer detailed explanations, contact email, phone, postal addresses and so on.

An Actual Scam

Here is an email the author received recently. See if it fits some of the preceding patterns.

> Subject: Compliments
> Date: Sat, 3 May 2025 09:10:09 -0700
> From: Gordon Cole KC <gorcole@gordoncole.co.uk>
> Reply-To: gordoncole@gordoncole.co.uk
> Compliments!
> I'm pleased to meet you.
> My name is Gordon Cole KC. I am a solicitor and investment adviser to your late relative, who left behind a substantial sum of money in a capital and investment security account, along with property documents. Given your familial connection through lineage, surname, and country of origin, I would like to discuss this claim with you.
> For further details, please kindly provide me with the following information:
>
> | | |
> |---|---|
> | Full name | Recent address |
> | Active mobile number | Age |
> | Marital status | Occupation |
>
> I look forward to your prompt response. Please send your full information to my private email: gordoncole@gordoncole.co.uk.
> Regards,
>
> Gordon Cole KC

Reporting Scams and Cyber Attacks

Alerted by tell-tale signs, you can simply dismiss the attempted scam and move on. Better yet, you can report it to relevant authorities. Let's list where you can report scams and attacks in the US:

- **General Online Fraud or Scams**—Federal Trade Commission (FTC) `reportfraud.ftc.gov`; Better Business Bureau `www.bbb.org/scamtracker`.
- **Internet and Cybercrime**—FBI (IC3) `www.ic3.gov` Internet Crime Complaint Center; US-CERT `phishing-report@us-cert.gov`.
- **Financial Fraud / Credit Issues**—Consumer Financial Protection Bureau (CFPB) `www.consumerfinance.gov/complaint`; Experian `experian.com /fraud`; Equifax `www.equifax.com/personal/credit-report-services`; TransUnion `transunion.com/fraud-victim-resource/place-fraud-alert`.
- **Phishing or Email Scams**—Gmail Use *Report phishing* from the drop-down menu; Outlook/Hotmail email `phishing@office365.microsoft.com`; Yahoo email `reportphish@yahoo-inc.com`.
- **Phone and Text Scams**—FCC `consumercomplaints.fcc.gov` Consumer Complaints.
- **Local or Regional Reporting**—Ohio `www.ohioattorneygeneral.gov` Attorney General's Office; Local Police Department.

Reporting a scam takes time and energy. But, we all should chip in to make cyberspace safer, to prevent others from falling victim, and to help isolate/arrest the devious scammers.

Computational Thinking as a Perfect Antidote

Today cyber scammers can hide behind the vast worldwide networks, yet their main scheme and technique is rather simple and centuries old—exploiting human vulnerabilities: wishes for good fortune, romance, getting goods/services for free, greed, desperation, gullibility, and desire for grandeur. History is filled with emperors who fell for eternal-life-on-earth scams!

Furthermore, cyber attackers count on people's habitual/compulsive clicking, lack of understanding of communication protocols, and blind trust in authentic looking messages/websites.

As we know, **Computational Thinking** promotes familiarity with the digital world, logical thinking, and paying attention to facts and details. In addition, CT trains us to follow well-designed procedures precisely and to anticipate forks in the road with preplanned reactions. Therefore, **CT can be the perfect antidote** to defeat all kinds of scams, especially the online variety. Thus, CT should be part of literacy in the digital age. Would you agree?