1. Phishing scams

Lucky you! A Nigerian prince has selected you to help smuggle millions out of his country. For a little bit of effort —a few simple wire transfers —you'll get a substantial cut. What could be easier?

I bet you're asking yourself, "Who would fall for that?" Well, tens of thousands of people do every year. That's why Nigerian scams, known as 419 scams, are still very popular.

Other versions might say you won a contest or have a job offer. Maybe someone wants to meet you, or you can make money for shipping some goods.

The catch is that you have to send in personal or banking information, or pay a fee. Of course, your information and money is going straight to hackers.

Use common sense before reacting to any e-mail. Scams rely on making you act quickly. If you think about things long enough, you can usually see through them. Just remember the old saying, "If it looks too good to be true …"

2. Trojan horse

Many hackers want to slip a virus on your computer. Once installed, a virus can record everything you type and send it back to the hacker. It can send out spam e-mail or attack other computers.

To do this, the hackers disguise the virus as something harmless. This is called a Trojan horse, or just Trojan.

One of the most popular ways to deliver a Trojan is a variation of the phishing e-mail scams.

For example, the e-mail might say it's from a shipping service, bank or other reputable company. There's been a problem with a transaction! To learn more, you have to open an e-mail attachment.

The attachment might look like a normal file, but it really contains a Trojan. Clicking on the file installs it before you can do anything.

Similar scams appear on Facebook and Twitter. You think you're going to watch a funny video your friend posted. Instead, a popup tells you to update your video player. The "update" file it provides is really a Trojan.

The key to defeat this tactic, as with phishing e-mails, is common sense. However, up-to-date security software is essential as well. It should detect and stop most Trojans before they can install.

3. Drive-by downloads

Security software is good, but it isn't always enough. Programs on your computer might have weaknesses that hackers can use to bypass security software.

To take advantage of these weaknesses, hackers set up websites embedded with viruses. You might get there by clicking a malicious link in a phishing e-mail or on social media. You can even find these sites in a search for popular programs or topics.

It isn't just malicious sites, though. Hackers can sneak malicious code on to legitimate websites. The code scans your computers for security holes. If it finds one, a virus can download and install without you doing anything.

To stay safe, you have to keep your programs up-to-date. Every month, Microsoft releases updates for Windows and Internet Explorer. These updates close critical security holes that hackers exploit.

Other critical programs to patch are Adobe's Flash and Reader, and Oracle's Java. Using old versions of these programs is like sending hackers an engraved invitation.

You should also be using the latest version of your programs. Anyone using Internet Explorer 6, 7 or 8 needs to update or switch browsers immediately.

4. Bypassing passwords

In Hollywood movies, hackers are masters of guessing account passwords. In the real world, however, very few hackers bother.

Instead, they go around passwords. They might get your password from a data breach at a company or website you use.

It's important that you use a different password for every account. That way, if a hacker discovers one, they can't get in to every account.

Perhaps the hacker slipped a virus on to your system. It records your passwords and sends them to the hacker; no guessing needed.

As I mentioned above, you can stop viruses with up-to-date security software and programs.

A hacker might tackle your account's security question. Most security questions can be answered with information people post publicly.

You should change how you answer security questions. Give a random answer that has nothing to do with the question. That way, no one can guess it.

5. Using open Wi-Fi

I'm sure you have a Wi-Fi network at home. Is it encrypted? If you don't know the answer, then it's probably, "no."

That means hackers, and neighbors, can connect to your network from outside. They can see and record everything you do. They can surf to bad websites and download illegal files on your connection. You might be getting a visit from the police.

You need to take a few minutes and secure your network. Trust me; it's worth it. The instructions will be in your Wi-Fi router's manual.

6. Social Engineering

Social engineering is a technique hackers use to manipulate end users and obtain information about an organization or computer systems. In order to protect their networks, IT security professionals need to understand social engineering, who is targeted, and how social engineering attacks are orchestrated.

7. Brute Forcing

Probably the oldest technique out there, Brute forcing involves trying permutations and combinations of characters from a particular character set.

For instance, if a hacker must crack the password of a file. He will try all combinations for a given length and then move to the next length.

So a hacker will try all characters like A-Z, a-z, 0-9 and special characters for length 1. If the password doesn’ t match the hacker will move to length 1 and again try all combinations. This technique is no longer viable for online attacks but is still effective for offline attacks.

8. MITM

Man in the Middle better known as MITM attack is a type of attack in which an intermediate device handles all requests that are made from it to a server.

In MITM attacks the hacker can :

Replace your Downloaded file with any other file.

Redirect you to other websites.

View all your browsing and typing history.

Connect to your phone if any ports are open.

MITM attacks usually take place in public places that offer Wi-Fi services like Coffee shops, Railway Stations, Restaurants, Libraries etc.

You may not want to use sensitive websites in public Wi-Fi zones as a measure of protection against MITM.

9. Keylogging

This is where it all began. The eldest and widely used method for hacking people. Keylogging is the process of creating a log(record) of all typed keystrokes on a system. All this data is then sent to the hacker' s server periodically.

Modern Keyloggers provide features like snapshotting the victim' s screen and even hide within other processes to not get detected.

10. Cookie Stealing

Cookies are used on almost every website around the internet. They are used to identify, remember and authenticate a particular user from the billions of other users on the website.

In Cookie stealing a hacker gains access to Cookies on your computer and imports them to his Browser.

So the next time he opens that particular site, the website will identify him as you and he has successfully stolen your identity. He will now do whatever illegal activities he wants and you will be blamed for the same.