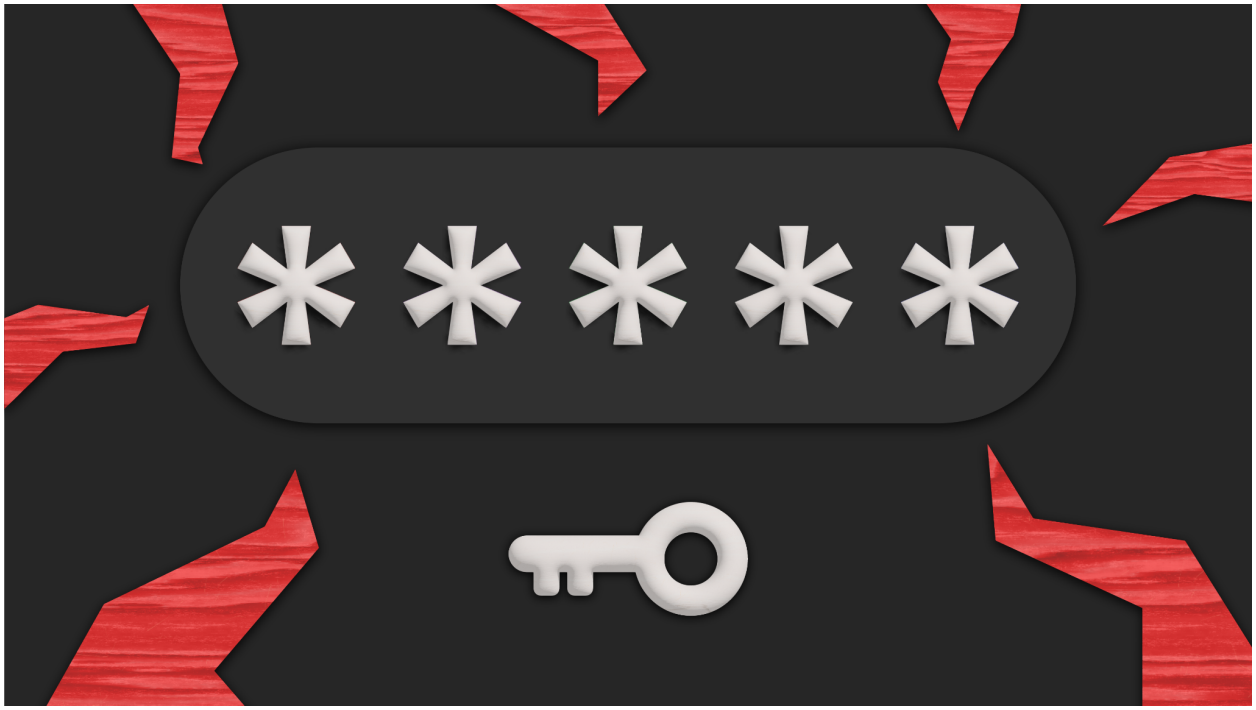


Password Breaches and Prevention

How are Passwords Hacked?

Passwords are bypassed through the use of password cracking tools, scamming techniques, and other methods of social engineering which involves the victim being duped.

The attacker does not need direct access to a victim's device, nor their PII (personal identifiable information). An attacker only has to use social skills, such as asking nicely, for an unaware person to deliver the requested information effortlessly.

Social engineering attacks are difficult to circumvent due to the craftiness of modern attackers. These include, but are not limited to;

1. Phishing
    a. Smishing
    b. Whaling
2. Pretexting
3. Business Email Compromise
4. Baiting

5. Scareware

1. **Phishing**
   Phishing attacks are those that target victims for personal identifying information.

   The goal is for the attacker to manipulate the victim into releasing crucial information, critical to business security and personal security. This usually pertains to social media, finances and other assets.

   Phishing attacks are usually done through email, but can also be carried-out through other communication-focused platforms.

   a. **Smishing** is a branch of phishing which involves the attacker disguising themself as a reputable organization.

      Smishing is derived from the combination of '*SMS'* and '*Phishing'*.

      This disguise is used to pry personal data from the victims being pursued. If the social engineering attack is successful, the victim releases enough data that will be useful toward the attacker's agenda.

   b. **Whaling** is a high value target (HVT) phishing attack pinpointed at executive level personnel.

      The derivation of Whaling is from the idea of executive personnel being viewed as the 'big fish', a.k.a., the 'Moby Dick' of the group. That being cyber terminology connecting the story of Moby Dick to the hierarchy in the workplace.

      These attacks are done to gain clearance to high level company data and analytics. Whaling is the most high-risk phishing attack since the targeted HVTs typically have access to most of the company's infrastructure.

2. **Pretexting**
   Pretexting is a social engineering attack where the attacker pretends to be a trusted official, family member or friend of the victim being scammed.

   Through external means, the attacker has acquired background information on the victim to know some of their real-world connections and relationships to carry-out this attack.

Social platforms including Facebook and Instagram makes it easy for attackers to find people and map-out connections.

Pretexting has a high likelihood of success, for the reason that most people don't expect a fraudulent account to pose as an official, family member, or under an alias of a friend.

3. **Business Email Compromise (BEC)**
   The Business Email Compromise can be seen as a more advanced form of pretexting.

   The attacker can use a multitude of tools to provide false-legitimacy to the victim. Spoofing and malware usage are some techniques that go into making a BEC attack successful.

   Spoofing may be the most hazardous method an attacker can use. Spoofing is an actor falsely identifying as someone, or something, they are not to gain trust, or access, they would not have otherwise.

   It's easy to overlook the slight variations done in the email header. That combined with malware, and/or counterfeit links, increases the risk factor. Two threat instances would be:

   a. A **fraudulent email**, sent from a feigned billing company, advising the customer/company to transfer payments to a makeshift website.

   b. The attacker pretends (**spoofing**) to be a supervisor for a company, deeming it a requirement that employees make purchases from a specified vendor.

4. **Baiting**
   Baiting is an attack used to persuade targets into falling for malicious media. Baiting is done in two ways; it can be done digitally, or physically.

   Digital baiting refers to media sent over the internet. Attachments are put together and forwarded to targets, marked as important documents, or luring media files. These files are typically embedded with malware capable of harming a user's device, as well as stealing personal information.

Physical baiting involves the attacker transmitting a materialized storage device to a target, in hopes that the target connects this device to their system. The physical devices used to bait include: CDs, USBs, SD cards and SIM cards.

This would give the attacker access to private information of the company/individual, and there is the potentiality of the malicious software spreading further to nearby systems devices.

Malware can spread through a variety of ways, but it's easily transferred through unaware individuals forwarding corrupted files, or corrupted devices, to other employees.

5. **Scareware**

Scareware is a tactic of using fear to manipulate targets into disclosing private information, downloading hazardous material or even to visit unsafe websites.

Think back to those random phone calls you get every once in a while.
The caller usually says something like:

> "*Hi, the deadline to pay your student loans has passed. Please provide your name and social security number to update your account on-file and prevent interest from being charged to your account.*"

This is a simple scare tactic that doesn't always work, but can be detrimentally abrasive once it does.

A more advanced scare tactic is giving a user a time-limit to complete an objective, or threaten a penalty if not followed.

For instance, while browsing unsecure web pages, a message box can pop-up that says,

> *"Your system has been compromised! Click this link now to begin securing your computer from leaking your password information from the most recent websites you have visited!"*

A 5-minute countdown would follow after the message.

One who is aware of cyber scams can easily ignore a pop-up as such, but some attackers have ways of proving themselves as 'reliable entities' throughout the scamming process.

This may be by way of including a phone number for a one-on-one call, or even providing a professional title that's false.

Nonetheless, all encounters have something a little different which makes every encounter just a little more unique than the last.

Scareware can also involve threatening the targeted victim—via phone call, messaging, or the web—to pay a ransom to retain the privacy of their information if attackers are able to gain access to their data.

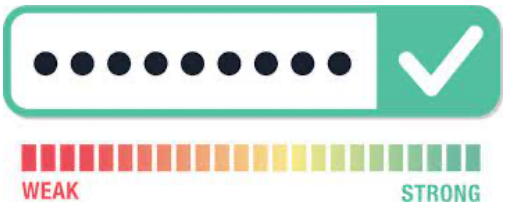
Attackers can **easily** exfiltrate user or company passwords through scareware.

They can either convince the target into releasing this information, or simply extract critical data through the use of their malicious software; that is if the target downloads these files. This is a huge issue for personal security and business security since the stakes are always high.

How Can this be Avoided?

The most strategic way of combating password breaches is by remaining updated on new methods cyber criminals are using.

It's always a good move for a company, or an individual, to expand their knowledge on threats to their personal security.



(SpyCloud, n.d)

A few great organizations that promote cyber-awareness are CISA, Foreign Policy, and Security Magazine.

They provide procedural updates on new cyber threats, and tech updates, as well as they offer a plethora of material on conflicting interests within the realm of cybersecurity and diplomacy.

Bibliography

Datto Security. 2022. “Common Types of Social Engineering Attacks.” Blog. https://www.datto.com/blog/common-types-of-social-engineering-attacks?utm_medium=opengraph&utm_source=225.

Federal Bureau of Investigation. N.d “Business Email Compromise.” https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise.

Kaspersky. 2022. “What Is Smishing and How to Defend Against It?,” https://usa.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it.

Nation Cyber Security Centre. 2020. “Whaling: How It Works, and What Your Organisation Can Do about It.” https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it.

Snelling, David. 2021. “Billions of Passwords Leaked! Check Here to See If You’re Affected.” Express.co.uk. https://www.express.co.uk/life-style/science-technology/1447711/Billions-passwords-leaked-online-RockYou2021.

SpyCloud. N.d. “Password Security Guidelines: Everything You Need to Know.” https://spycloud.com/solutions/password-security/.