The Art of Password Theft

Shoulder Surfing

No one likes a lurker.

It always pays to be aware of your surroundings so no one is able to observe you typing your password.

Brute Force

Next time you get locked out of your account for using the wrong password, be glad.

Some programs are capable of guessing billions of passwords until the correct one is found.

Social Traps

Not convinced by the Nigerian princess offering you a cargo-ship full of gold?

Social engineering techniques trick people into revealing their passwords, often playing off trust and curiosity by using compelling stories and familiar names.

Old-Fashion Theft

Did it really seem like a good idea to write your password on a post-it note and stick it under your keyboard?

Insecurely stored passwords can be stolen - *this includes handwritten passwords hidden close to a device.*

A Guessing Game

Are your birthday, anniversary, and maiden name displayed on your social media profile?

Easy to remember passwords based on personal information such as names, important dates, and addresses can also be easy to guess.

Searching

Remember when your browser asked if you wanted to store your password and you said, "heck yes?"

Your IT infrastructure can be searched for electronically stored password information.

Interception

Free Wifi? Sign me up! Or don't...

Passwords can be intercepted as they are transmitted over an unsecured network.

Key Logging

Next time you consider clicking on a suspicious link, remember what curiosity did to the cat.

Once installed, a keylogger can intercept passwords as they are being typed.

So what can you do about it?

Don't store passwords in plain text format. *Or on scraps of paper within reach of your devices...*

Leverage account lockout and monitoring to help prevent brute force attacks.

Keep it secret, keep it safe. When it comes to sharing passwords, the correct choice is simply *don't.*

Say no to obvious and common password choices. *i.e. 12345, password, qwerty, or personal information such as birthdays, anniversaries and names.*

Change your password proactively. Whether you fall under the "90 day" camp or not, be mindful of the strength and duration of your password, and don't hesitate to reset it if you feel there is a possibility of compromise.

Don't use the same password on multiple accounts. This can create a domino effect that allows hackers to take down multiple accounts by just cracking a single password.

Use Two-Factor Authentication. By using 2FA as an additional layer of protection you can significantly decrease the risk of an attacker gaining access to your online accounts.

To learn more about leveraging technology to protect and optimize your business, contact us at ***hello@seedspark.com*** or visit us at ***www.seedspark.com***