5 Simple Steps to Ruining a Hackers Day

TSP Technology, Inc.

www.tsptechnology.com

503-208-7430

Step 1: Enforce Long Passwords of 21 Characters or More*

- Hackers use techniques such as Password Spraying to try common password (such as Spring2022!) across multiple user accounts
- Most SMB's (Small & Medium Businesses) have no password policy configured and enforced
- The time it takes to compromise or crack passwords of 7 characters or less is less than a few minutes
- ***Every single character that you add doubles the time required to crack***
- Password Policies requiring 21 characters using passphrases (at least 1 number and 1 special character) are easy to remember and will require billions of years to crack

Step 2: Block All Browser Ads*

- The internet is very large and most of it is used for evil (Dark web). Browser Ads show often show up when searching for something on Google, mimicking real search results. However, they are regularly exploited by hackers to redirect you to a malicious website.
- The simplest way to prevent this is by using an alternative browser like Brave (can be downloaded at brave.com), which has a similar look and feel to Google Chrome but will block ads and has built in privacy protections.

Step 3: Turn on Two-Factor Authentication for Email*

- Whether you use Gmail or Microsoft Office365, your account can be compromised without you even realizing it. The only thing they need is your username and a password.
- If a hacker gains access, they will quickly send out emails (with malicious attachments) to your entire contact list. This remains their number one favorite method of attack.
- Two-Factor Authentication will send a text to your phone verifying you are the one logging into the account. This will effectively stop the attackers in their tracks and prevent the account from being compromised.

Step 4: Segment Your Network Computers*

- Configure Windows Defender Firewall with Public Network settings (like you're in a coffee shop) to block all inbound connections.
- Many Anti-Virus products have a built in Firewall which should be turned on if you have one
- The goal is to stop Lateral Movement by hackers once a system is compromised

Step 5: Remove Your User Account from the Administrators Group*

- Computers are designed with tiered permission levels for accomplishing tasks. As an administrator, you have full reign over the entire system and can do whatever you want. Hackers will use this to their full advantage.
- There should only be one or two administrator accounts on the computer, and it should only be used for authenticating when required (i.e downloading company software). Other accounts should be left out of the administrator group.

*If you are a part of a domain-controlled organization, you may need to reach out to your IT department to make some of the above changes.

Interested in even more steps you can take to ruin a hacker's day? Contact us to learn how to implement things such as:

- Web and DNS Filtering
- Intrusion Detection and Prevention
- Advanced Endpoint Protection
- Application and User Control
- Enabling Sysmon for improved logging
- 24/7 Security Operations Center
- Private VLAN's
- Regular Vulnerability Scans
- Two Factor Authentication for Computers, VPNs, Network Firewalls, etc.