Cybercrime damages set to cost the world $6 trillion annually by 2021

Ransomware

Ransomware is a type of malware that blocks access to a victim's assets and demands money to restore that access. The malicious software may either encrypt the user's hard drive or the user's files until a ransom is paid. This payment is typically requested in the form of an encrypted digital currency, such as bitcoin. Like other types of malware, ransomware can spread through email attachments, operating system exploits, infected software, infected external storage devices, and compromised websites, although a growing number of ransomware attacks use remote desktop protocols (RDP). The motive for these types of attacks is usually monetary.

Why is ransomware a threat that continues to spread like wildfire? Simple: it's easy for cybercriminals to access toolsets. Ransomware-as-a-Service (RaaS) sites make it extremely easy for less skilled or programming-savvy criminals to simply subscribe to the malware, encryption, and ransom collection services necessary to run an attack—and fast. Since many users and organizations are willing to pay to get their data back, even people with little or no technical skill can quickly generate thousands of dollars in extorted income. In addition, the cryptocurrency that criminals demand as payment, while volatile in price, has seen huge boosts in value year over year.

Tips to combat ransomware:

- Keep company operating systems and application patches up-to-date.
- Use quality endpoint protection software.
- Regularly back up company files and plan for the worst-case scenario: total data and systems loss (consider business continuity if budgets allow).
- Run regular cybersecurity trainings with employees and clients.

Phishing

Phishing is the attempt to obtain sensitive information, such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information into a fake website, the look and feel of which are almost identical to a trusted, legitimate site.
Phishing is a common example of a social engineering attack. Social engineering is the art of tricking or manipulating a user into giving up sensitive or confidential information. The main purpose of a phishing attack can range from conning the recipient into sharing personal or financial information, to clicking on a link that installs malware and infects the device (for example, ransomware uses phishing as its primary infection route.)

Tips to combat phishing:

- Ensure your employees and clients understand what a phishing email looks like and how to avoid becoming a victim by testing your users regularly. Train them with relevant phishing scam simulations.
- Hover over URLs in email to see the real address before clicking.
- Use endpoint security with built-in anti-phishing protection.
- Consider a DNS filtering solution to stop known phishing and malicious internet traffic requests.

Brute Force Attack

A brute force attack is a cyberattack in which the strength of computer and software resources are used to overwhelm security defenses via the speed and/or frequency of the attack. Brute force attacks can also be executed by algorithmically attempting all combinations of login options until a successful one is found.

It's important to note that brute force attacks are on the rise. Earlier this year, Rene Millman of SC Magazine UK reported, "hacking attempts using brute force or dictionary attacks increased 400 percent in 2017."

Tips to combat brute force attacks:

- Scan your systems for password-protected applications and ensure they are not set to default login credentials. And, if they're not actively in use, get rid of them.
- Adjust the account lockout policy to use progressive delay lockouts, so a dictionary or brute force combination attack is impossible.
- Consider deploying a CAPTCHA stage to prevent automated dictionary attacks.
- Enforce strong passwords and 2-factor authentication whenever possible.
- Upgrade your toolset. RDP brute force is a major ongoing issue. Standard RDP is highly risky, but secure VPN paid-for alternatives make remote access much more secure.