networkdoctor
IT SOLUTIONS & SERVICES

CYBER ATTACKS

ARE AT AN ALL-TIME HIGH

THE MOST COMMON AND HARMFUL ATTACKS ARE:

RANSOMWARE

Encrypts your files making them unusable. Victims must pay a ransom to receive a decryption key.

EMAIL BREACHES

Mailboxes are accessed in order to impersonate a user and scam contacts into sending funds or steal contact information.

More than **4,000** ransomware attacks occur every day.

80% of breaches contained customer PII.

Damage related to cybercrime is projected to hit **$6 trillion** annually by 2021.

THE BEST WAY TO FIGHT THESE ATTEMPTS:

- **DETECT AND ALERT**
- **PREVENT AND MITIGATE COLLATERAL DAMAGE**
- **EDUCATE**

Network Doctor has assembled a mix of solutions and best practices to protect clients:

- **INTRUSION DETECTION AND PREVENTION SOLUTION (IDS / IPS)**
  - Agents are installed on workstations, servers, and LAN. Using artificial intelligence, if unusual behavior is detected, such as mass encryption of files, connections will be severed to prevent the infection of other devices on the network.
  - Networks are monitored for suspicious files and activity 24/7 by a SOC staffed with security engineers. If detected, action will be taken immediately.
- **EMAIL ACCESS ALERTING**
  - Monitors Microsoft 365 Account's audit logs for suspicious activity, such as logins from other countries or the creation of unusual mail-forwarding rules.
  - Upon receipt of an alert, our support team will take action to ensure unauthorized access is severed.
- **EDUCATION AND TRAINING**
  - Continually educating users on best practices to keep safe is one of the most effective ways to prevent breaches.
  - Solutions to identify users with weak security habits are available.