How Cybercriminals Are Targeting Your Small/Medium-size Business

And How We Can Help Protect Your Business

happier IT®

1-in-5 Canadian SMBs have been affected by a Cyberattack or data breach in the last two years.

INSURANCE BUREAU OF CANADA

Canadian Businesses are losing more than $3 Billion a year to Cybercrime.

CANADIAN CENTRE FOR STRATEGIC AND INTERNATIONAL STUDIES

Canada saw a substantial (170%) rise in phishing volume between from April 2018 and April 2019.

PHISHLABS - 2019 PHISHING TRENDS AND INTELLIGENCE REPORT

Why Cybercriminals Target Small/Medium-sized Businesses

happier IT®

This is not the Cyber Criminal of Today

Cybercriminals Today

- Anyone can be a cyber criminal today
- Darkweb makes it easy for amateur cyber criminals to buy tools
  - Ransomware-as-a-Service available free with profit-share or as low as $50
- Darkweb and sell stolen
  - Credit Cards
  - Banking Information
  - Credentials
  - Malware Infected PCs
- Cybercrime organizations have hundreds of employees
- Often paid salary + bonuses based on revenue generated
- Different departments including Training and Target Research
- Highly sophisticated
- Some resell as-a-Service tools to amateur cyber criminals

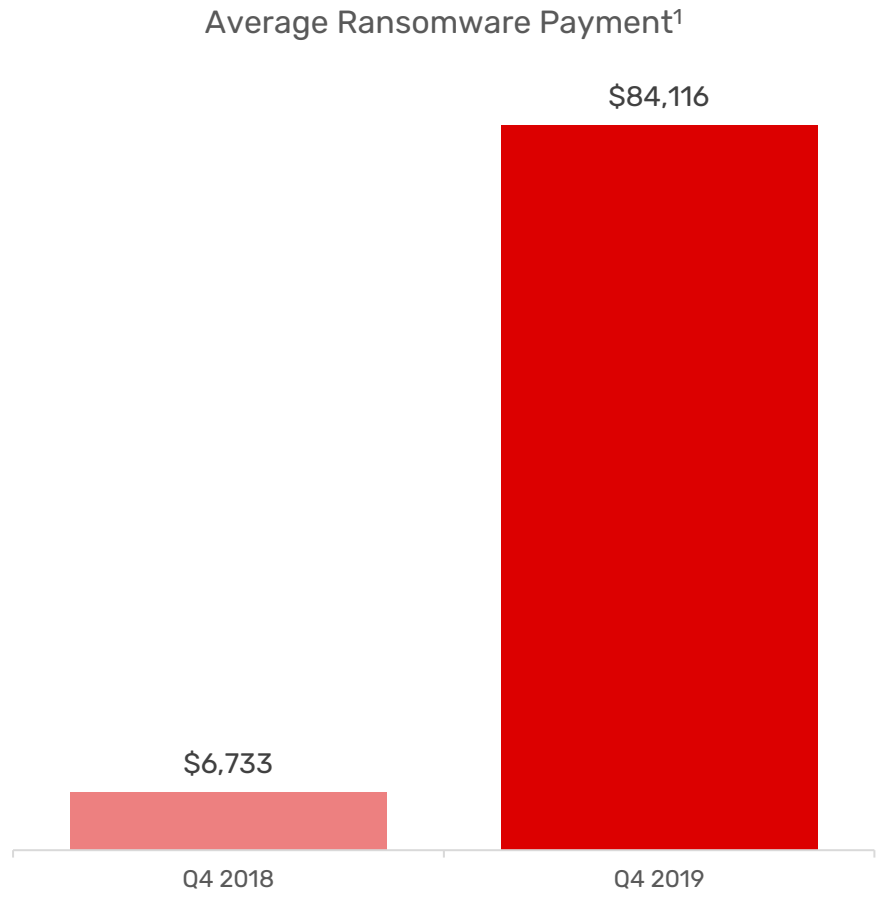
happier IT®

Most Common Types of Cybercrime

happier IT®

Ransom

- Hold a Business, Organization or Government Ransom
- #1 Reason for Attack in 2019[1]
- 365% Increase in business detections of Ransomware from Q2 2018 to Q2 2019[2]
- The average Ransom payment increased 1150% from 2018 to 2019[1]



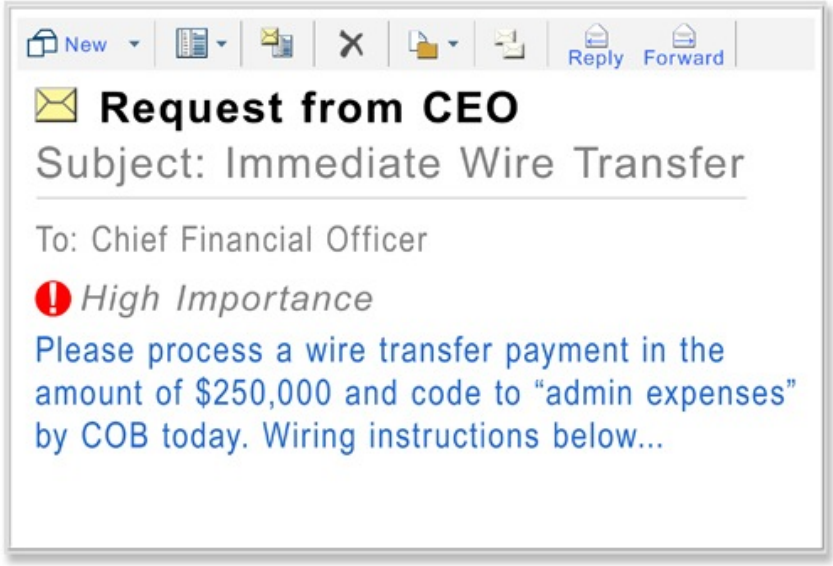
Sources

1. Coveware - Q4 2019 Ransomware Study
2. MalwareBytes – Cybercrime Tactics and Techniques

happier IT®

Imposter Scams

- Fraudulent Accounts Receivable
- Executive Wire Transfer
- Gift Card / Prepaid Credit Card



Theft of Information

- Personally Identifiable Information (PII)
  - Sold many times over on the dark web
- Credentials (email address/password)
  - Sold many times over on the dark web
- Intellectual Property / Trade Secrets
  - Highly targeted
  - Often outsourced to professional hacking groups
  - Sometimes State-funded (China/Russia)

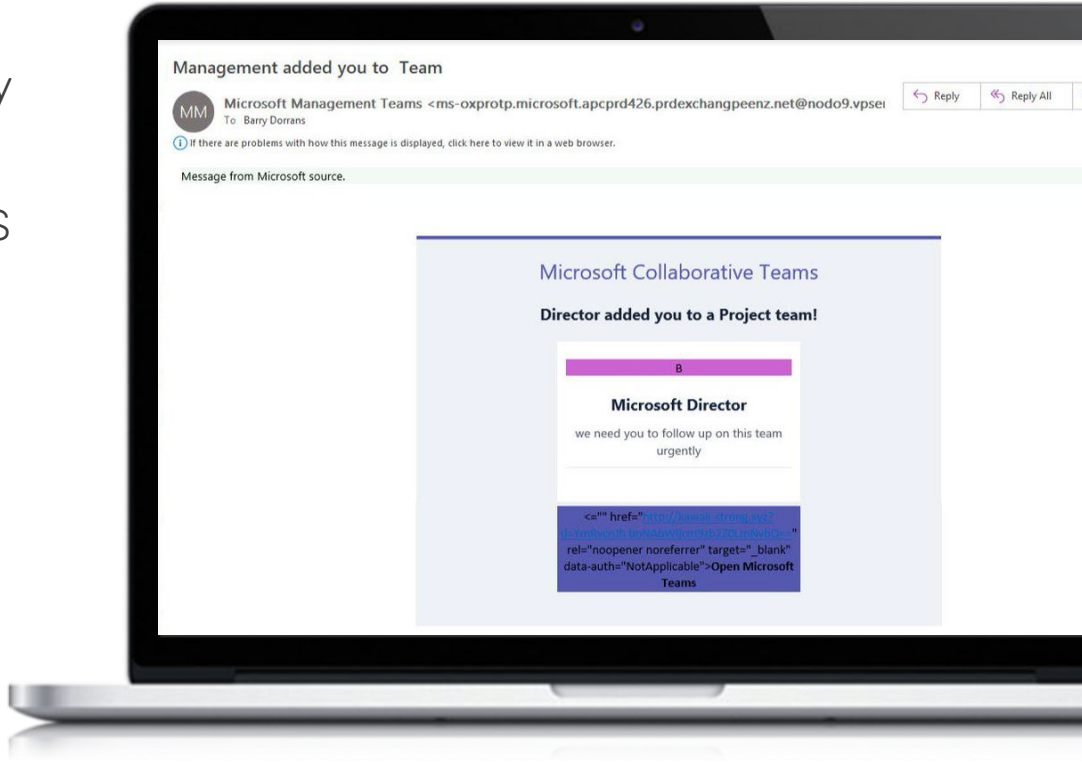
happier IT®

Most Common Cyberattacks Targeting Small/Medium-sized Businesses

happier IT®

Phishing

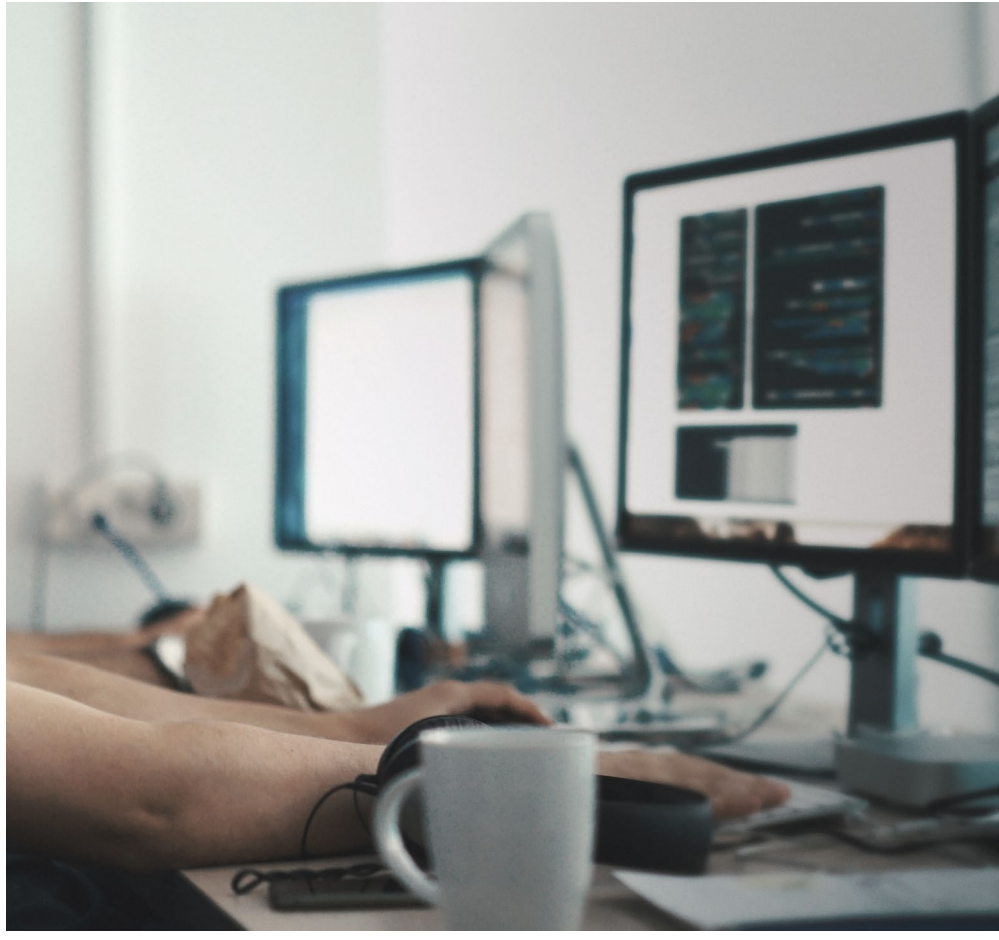
- Social engineering attack involving trickery
- Variants include “vishing” – attacks by telephone and “smishing” those using SMS or text
- Targeted phishing is “spear phishing”
- Cybercriminals Research and Carefully Choose their targets
- Typical objectives of Phishing
  - Trick Users into providing information of value
    - Credit Card or Banking Information
    - Credential Theft
  - Install Malware
  - Gain Access to Systems



happier IT®

Hacking

- Targeted Attack on Computer System
- Find Vulnerable Systems
  - Access gained through Phishing
  - Lists of vulnerable systems sold on Darkweb
  - Scanning themselves for vulnerable systems
  - Purchasing Compromised Credentials
- Gain Access
  - Vulnerabilities that bypass the need for credentials
  - Compromised Credentials
  - Brute Force Passwords using password list
- Dwell Time
  - 279 Days average to identify and contain a breach[1]
  - Hackers increasing “dwell” time (remaining hidden longer) on systems during attacks[2]



Sources

1. IBM Cost of a Data Breach Report 2019
2. CrowdStrike Services Cyber Front Lines Report 2019

happier IT®

Spyware

- Typically distributed through Phishing or Malicious (hacked) web-sites
- Installed by End-Users unknowingly
- Usually goes undetected by Antivirus
- Steals Information
  - PII Belonging to employees/customers/patients etc.
    - Social Insurance Numbers
    - Birth Dates
    - Medical Information
  - Steal Passwords
  - Steal Credit Card / Banking Information
    - Credit Card Numbers
    - Bank Account Numbers / Information
    - Online banking / payment system logins

happier IT®

Zombie Malware

- Typically distributed through Phishing or Malicious (hacked) web-sites
- Usually goes undetected by Antivirus
- Uses computer to conduct malicious actions
  - Sending spam/phishing emails
  - Participating in large coordinated attacks
  - Crypto-mining
- Potential Impact
  - Computer Performance Degradation
  - Wear that could lead to premature hardware failure
- Often sold as a means to deploy other malware like Ransomware once no longer useful

happier IT®

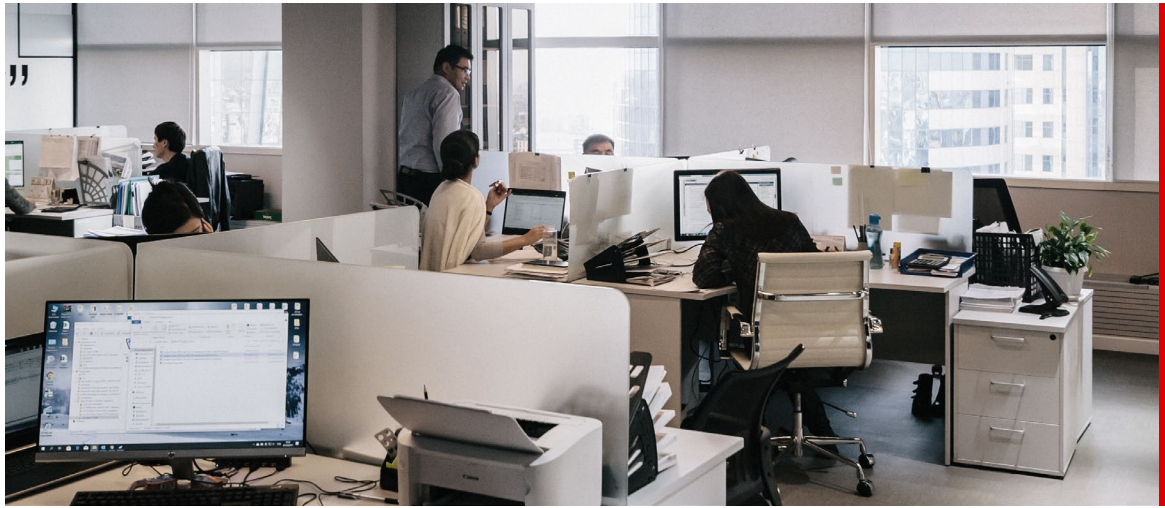
Ransomware

- Encrypts computers and any files they can access so they are unusable until Ransom is paid
- Usually spreads to every computer on the network
- Encryption is not reversable without paying ransom
- No guarantee the ransom payment will work
- Almost always used at the end of any cyber attack
- Hackers try to delete backups before installing Ransomware
- The cost of downtime inflicted by Ransomware was nearly 7.5X higher than the ransom[1]

Sources

1. Datto - 2019 State Of Ransomware Report

happier IT®



Cyber Security Is Critical To Your Business

happier IT®

Impact of a Cyberattack

- Attacks can be extremely costly and threaten the viability of your business
  - Direct costs
    - Ransom
    - Remediation Costs
    - Downtime
    - Legal costs
    - PR costs
    - Victim services
  - Indirect Costs
    - Reputation Damage / Loss of Trust with Customers/Employees
    - Lost opportunities
  - Compliance Issues
    - Regulatory penalties
- 60 Percent Of Small Companies Close Within 6 Months Of Being Hacked[1]

Sources

1. Cybercrime Magazine

happier IT®

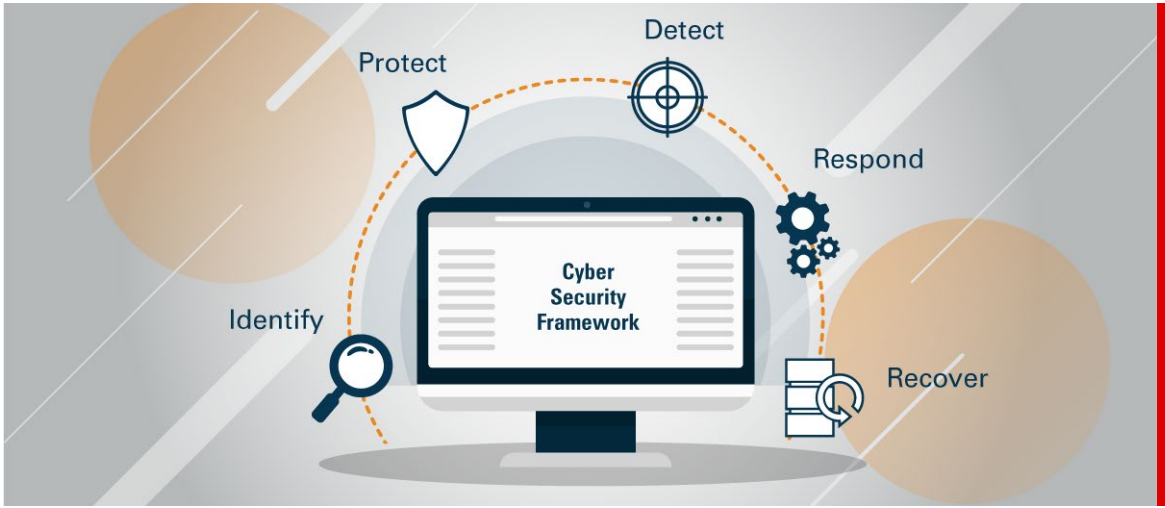
Likelihood of a Cyberattack

- Attackers see small businesses as easy targets
  - No dedicated in-house security team
  - Less budget/investment in security tools
  - Vulnerable to simpler attacks
- 1-in-5 Canadian SMBs have been affected by a Cyberattack or data breach in the last two years.[1]
- 1-in-4 chance your business will experience a Cyberattack this year.[2]

Sources

1. Insurance Bureau of Canada
2. Ponemon Institute

happier IT®

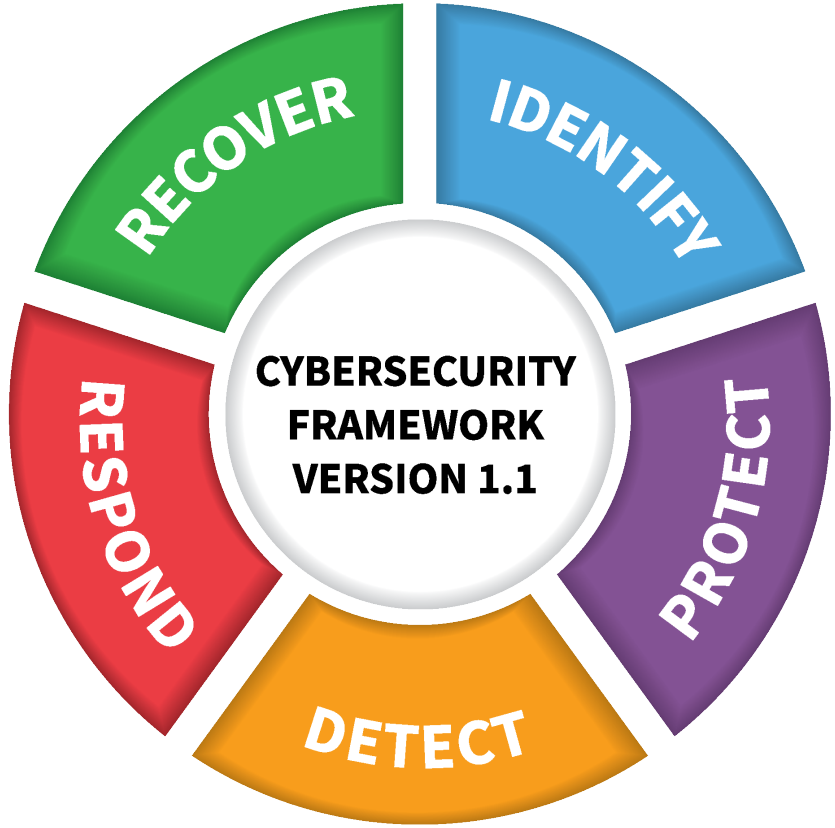


Cyber Security Frameworks & Standards

happier IT®

Frameworks

- Many frameworks available; We focus on two
- NIST Cyber Security Framework
  - Provides a continuous process for cybersecurity risk management
  - Gives structure, guidance and standardization to Cyber Security
- CIS Critical Security Controls
  - CIS is much more specific on Cyber Security controls
- Most organizations focus almost exclusively on Protect
- We offer NIST / CIS compliance assessments



happier IT®

Essential Solutions to Protect Against Today's Most Common Threats

happier IT®

Cyber Security

- No one-size-fits-all Cyber Security product
- No product works 100% of the time
- Layer protection and continually review
- Yesterdays protection may not protect against tomorrows threats
- The following are the fundamental protections every business should have
- Not a complete list – but have these in place before more advanced solutions

happier IT®

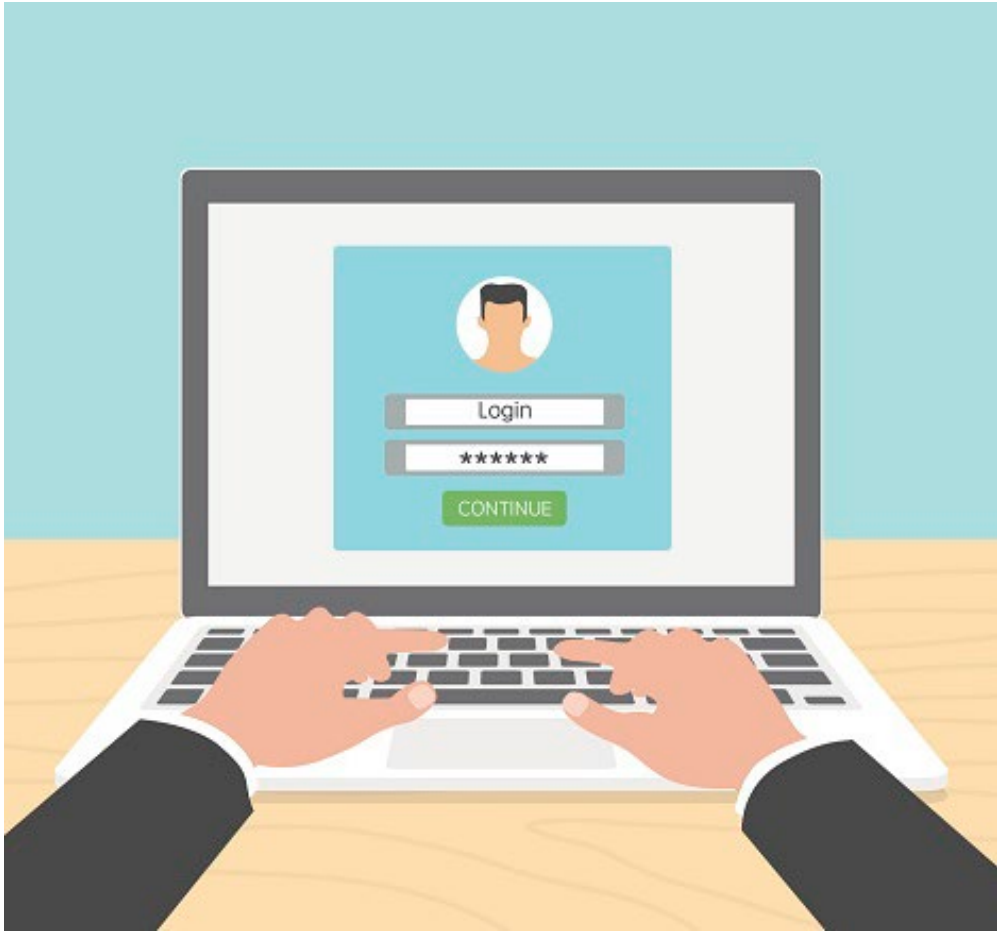
Phishing

- Implement Microsoft 365 Anti-phishing Policy (new June 2020)
- Implement Microsoft Office 365 Advanced Threat Protection
- Implement Cyber Security Awareness Training
- Implement DNS Filtering
  - Block known bad links/servers
  - Block spyware from exfiltrating data
  - Prevent Zombie Malware from being used

happier IT®

Hacking

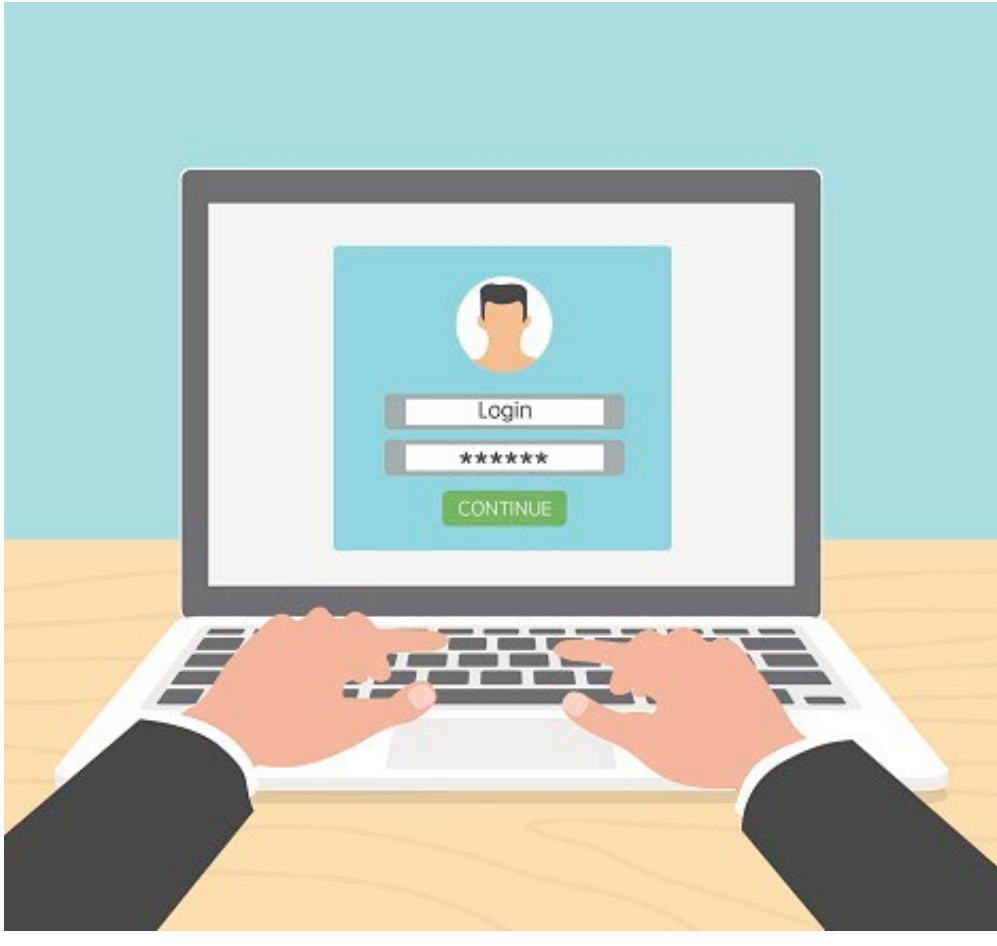
- Free things to reduce vulnerability to hacking
  - Enforce Password Policies (no exceptions)
  - Review & remove stale user accounts
  - Enable/Enforce Multi-factor Authentication on Office 365 and remote access
  - Restrict or close external connections (RDP / public web URLs)
  - Ensure no users have Local Administrator access (can install software)
  - Implement some software configuration changes on your network to prevent common attacks
- Protect against known vulnerabilities/exploits
  - Ensure OSs running supported version
  - Ensure hardware is replaced



happier IT®

Hacking (cont.)

- Segment your network
  - Ensure all SmartPhones and Devices that don't need server access use Public Wi-Fi (internet only)
  - Ensure all cameras, phones, and 3rd party vendor devices are on their own restricted network
- Scan for known vulnerabilities
  - Recommend having annual scan performed
  - Identifies vulnerable devices so they can be remediated or replaced
- Monitor for Compromised Credentials
  - Users often use the same password for multiple systems
  - Detects compromised credentials for sale on the dark web
  - Notifies your user so they can change their password at work or wherever else they use it



happier IT®

Hacking (cont.)

- Implement Managed Detection & Response
  - Collects logs and monitors activity
  - Looks for unusual behavior
  - Detects threats quickly and reduces dwell time
  - 24/7/365 SOC response & remediation of threats

happier IT®

Spyware / Malware

- Antivirus isn't enough
  - Often spyware and other malware is not identified by antivirus software
  - Traditional antivirus is based what a virus looks like
- DNS Filtering
  - Prevents your computer from talking to known malware sources and bad actors.
- SentinelOne - Advanced EndPoint Protection
  - Antivirus Replacement
  - Uses AI Behavioral Analysis to detect threats
  - Autonomous AI Protection self defends and heals
  - 24/7/365 SOC response & remediation of threats

happier IT®

Ransomware

- SentinelOne - Advanced EndPoint Protection
  - As discussed previously
  - Automated isolation to protect other devices
  - Patented file protection capability
  - Ransomware roll-back
  - $1M Ransomware Warranty
  - 24/7/365 SOC response & remediation of threats

happier IT®

Recovery

- There is always a risk that a threat will get through
- Protect On-premise Applications / Data
  - Many traditional backups are easily corrupted or erased by hackers
  - Datto Business Continuity
    - “Airlocked” system - can’t access backups from server
    - Stored on-site and in cloud
    - Can restore files encrypted by Ransomware
    - Can start a virtual version of the server in minutes
- Protect Microsoft 365 / G-Suite
  - Native data protection doesn’t protect against
    - Human Error
    - Programmatic Errors
    - Malicious Insiders
    - External Hackers
    - Viruses / Malware / Ransomware

happier IT®

Cyber Security Tips

- Be careful of email attachments, web links and voice calls from unknown numbers.
- Do not click on a link or open an attachment that you were not expecting.
- Use separate personal and business computers, mobile devices, and accounts.
- Use multi-factor authentication where offered.
- Do not download software from an unknown web page.
- Never give out your username or password.
- Consider using a password management application to store your passwords for you.

happier IT®