CAPE COD 5

Business Guide: Cybersecurity Awareness

5 Quick Tips

1. Regularly educate/reinforce established information security practices with staff.
2. Keep software updated and patched.
3. Periodically review physical and computer security control practices.
4. Utilize Cape Cod 5's Treasury Management Services to help mitigate and prevent account takeovers.
5. Be an ambassador – share this information with others.

Cyber Attacks

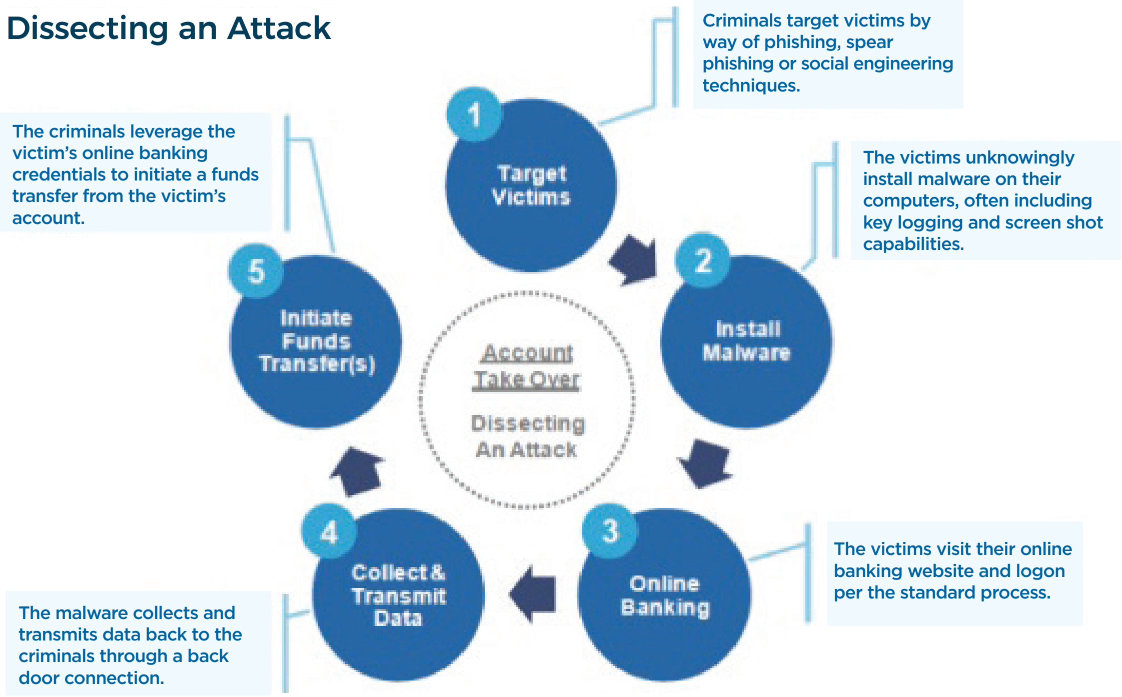
Current Environment

- More than $1.2 billion dollars in losses were suffered due to Business Email Compromises (BEC) in 2018.
- Every 40 seconds a business is hit with ransomware (up from every 2 minutes in 2016).
- 67% of businesses hit with ransomware permanently lost part or all of their data.
- Cloud storage is increasingly a target for cyber criminals in 2019, along with the use of machine learning and artificial intelligence (AI) to further automate the attacks.

The "How"

- Criminals target victims through social engineering campaigns such as phishing to conduct business email compromises and other credential harvesting opportunities.
- Criminals also access dark web databases that sell credentials from historical data breaches.
- Credentials are used to authenticate into your system to deploy malware and account takeover.
- Outdated software and missing patches can expose vulnerabilities to your current operating systems, making your network more susceptible to an attack.

Dissecting an Attack



Criminals target victims by way of phishing, spear phishing or social engineering techniques.

The victims unknowingly install malware on their computers, often including key logging and screen shot capabilities.

The victims visit their online banking website and logon per the standard process.

The malware collects and transmits data back to the criminals through a back door connection.

The criminals leverage the victim's online banking credentials to initiate a funds transfer from the victim's account.

Credit: FBI IC3 Advisory. Sources: Kaspersky, Federal Bureau of Investigation and Massachusetts Institute of Technology

Continued on back

CAPE COD 5 **Business Guide: Cybersecurity Awareness**

Continued from front

Key Practices to Protect Your Business

- Krebs's 3 Rules for computer safety (Brian Krebs - Krebsonsecurity)
  - If you didn't go looking for it, don't install it.
  - If you installed it, update it.
  - If you no longer need it, get rid of it.
- Regularly back up data. Know where your data is stored if using Cloud.
- Create tiered access rights for employees based on job function.
- Document information security procedures, including how to safely dispose of physical and electronic files and old devices. Also document a response plan in the event of a data breach.
- Train staff on information security procedures, including the cost of non-compliance - money and reputation.
- Include any third parties/vendors with access to your data as part of your information security plan.
- Protect your bank accounts:
  - Isolate machine(s) used for business and online banking from internet browsing.
  - Utilize CC5 Treasury Management services such as business online banking, Positive Pay and ACH debit blocker to proactively protect your bank accounts.

How to Respond if Breached

- **CONTAIN**
  - If compromised, disconnect infected devices from your network.
  - Notify financial institutions to protect bank accounts.
- **ERADICATE**
  - Professionally clean compromised devices.
- **RECOVER**
  - Restore data from back-ups.
- **NOTIFY**
  - Make law enforcement aware – local and FBI Internet Crime Complaint Center (IC3).
  - Notify staff and customers.
- **REVIEW**
  - Look at existing controls and make modifications as necessary.
  - Retrain staff.

Resources:

- FTC Cybersecurity for Small Business:
  - **www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity**
- FBI Internet Crime Complaint Center (IC3):
  - **www.ic3.gov**
  - **www.krebsonsecurity.com**