ATOMICdata

QUICK GUIDE

PHISHING AWARENESS

Phishing comes in many forms, and even the most vigilant of users can be fooled. That's why everyone in a company must stay up to date with the most popular social engineering tactics.

$7.35 MIL
Average total organizational cost of a data breach in US[1]

43%
Percentage of 2016 data breaches resulting from phishing[2]

TYPES OF PHISHING

High ranking executives have cyber-bullseyes on their backs. All any malicious actor needs to start an attack is a name and company. This is called Spear Phishing.

SPEAR PHISHING Personalized email attack using publicly available information. Attackers will attempt to procure your credentials and emails may include links/attachments that will download malicious programs like ransomware or keyloggers.

RANSOMWARE Malware that encrypts data on a machine or network of machines and demands payment to decrypt the data.

KEYLOGGERS Software that may hide in an operating system, intercept and log keystrokes to steal confidential information like usernames and passwords.

HOW TO PROTECT YOURSELF

- **BE SUSPICIOUS** Hover over links before clicking on links embedded in emails. This will show the actual destination of a hyperlink. IP addresses are a red flag!
- **TRUST YOUR GUT** If an email looks "off" or "weird" it probably is. Look for misspellings of common words or names, email addresses that look slightly different, and unnecessary urgency.
- **PLAY THINGS CLOSE TO THE VEST** Avoid posting personal information online. LinkedIn, Facebook, company websites or blogs; take care not to divulge information that could be used for social engineering.
- **KEEP IT CONFIDENTIAL** Never send confidential information over email (e.g. usernames and passwords).
- **USE BEST PRACTICES** Antivirus software, strong passwords, and consistent patching are foundational elements of IT security, regardless of your role or risk profile.

Cyber-criminals are smart, but not necessarily creative. Attack scenarios are used ad nauseam to gain access or information. Attackers will always be in a hurry - trying to frazzle you or your employees into making a quick, unthinking mistake.

$4.13 MIL
Average value of a company's lost business resulting from a breach[1]

80%
Percentage of breaches enabled by weak or stolen passwords[2]

WHO TO WATCH FOR

WIRE TRANSFERS & FRAUDULENT INVOICES Hackers will spoof emails from vendors, banks or billing departments asking for a wire transfer. Spoofed emails will attempt to get you to download attached malicious files or transfer money to bogus accounts.

EXECUTIVE/ATTORNEY IMPERSONATION Cyber-criminals will pretend to be executives or attorneys in your organization. They will use intimidation to pry info out of employees.

DATA THEFT Emails spoofed to imitate an executive asking Human Resources for W-2s or other personally identifiable information.

BAITING Lost USB flash drives, offers for free food, cheap vacations, and other tactics exploit human curiosity to gain credentials or access. If it seems too good to be true, it is.

HOW TO PROTECT YOUR COMPANY

IDENTIFY HIGH RISK USERS like C-suite executives, Attorneys, Accounting and IT administrators. These individuals must remain hyper-aware of cyber-attacks. **IMPLEMENT TECHNICAL CONTROLS** such as two-factor authentication, password policy enforcement, patch management, mail filtering, etc. **WRITE & USE A SECURITY POLICY**, agreed to by all employees. Including: mandatory annual security training, password management, acceptable use, etc. **PLAN FOR BACKUP, DR, & INCIDENT RESPONSE** Regularly scheduled backups and data retention, a disaster recovery policy, and a documented incident response plan must be in place. **TEST PHISHING AWARENESS** Phishing emails sent to employees on a regular basis by an internal or external IT security resource.

[1] Ponemon Institute Cost of Data Breach Study 2017, [2] Verizon, 2019 Data Breach Investigations Report. Revision June 14, 2018 10:26 AM.