Defend Your Business From Social Attacks

What are social attacks?

Social attacks target the human element of an organization. The goal of a social attack is to manipulate the target to divulge confidential information. Common social attacks are phishing and spear phishing.

What is phishing?

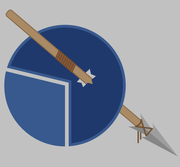
Phishing attacks are designed to trick someone into giving up their valuable information. A phishing attack can appear to be a routine email from HR, a client, your boss, etc.. Phishing attacks are most commonly carried out through email, but they can also occur through text and even phone calls.

It can happen to you!

64% of organizations have been the target of a phishing attack in the last year.

Source: Check Point Research Security Report

Spear phishing accounts for 71% of all targeted attacks!



Source: Symantec Internet Security Threat Report

What is spear phishing?

Phishing involves casting a wide net of relatively low effort attacks, while spear phishing targets fewer people with a more sophisticated attack. Spear phishers research and personalize their attacks to manipulate their targets. By tailoring their attacks, spear phishers have a higher success rate.

How to Defend Your Business

These are the 4 components of a secure IT environment:

- Employee Training
- Company IT Policy
- IT Security Software
- Routine Testing

Employee training has lowered the success rate of phishing attacks to

5%

Source: Enterprise Phishing Resiliency and Defense Report

Employee Training

Employees can either be a business' strongest defense or greatest liability. Without proper education and training, employees are more likely to become a victim of a social attack. Keeping employees up-to-date on security best practices can save your business from disaster.

Company IT Policy

Strong IT policies combined with set procedures reinforce employees' security training. It is critical for every business to have procedures that address a variety of predictable IT security scenarios. When a company is breached, time is critical; set procedures can help prevent further damage and expedite recovery.

IT Policy Example

Policy: "Nobody from within the company will ask you for your passwords through email."

Result: Employees will be less likely to fall for phishing emails disguised as an internal request.

IT Procedure Example

1. Employee receives suspicious email
2. Employee reports email to IT department
3. IT department warns company of phishing threat
4. IT department conducts audit to determine if there was a data breach

IT Security Software

Businesses can't solely rely on their security software. IT security software is most effective when your employees are trained on IT security principles and have company policies and procedures to support them. An example of security software that is effective against social attacks is Microsoft's Advanced Threat Protection (ATP).

Features of Microsoft's Advanced Threat Protection (ATP) that protect against social attacks:

Safe Links
When a potentially malicious link is clicked, ATP will intervene and warn the user that the link could be harmful.

Attachment Protection
ATP will scan for malware-infected attachments and will take action to protect your company.

Testing Best Practices

1. Have explicit goals before starting
2. Get the executive team involved
3. Choose 2 or 3 behaviors to shape and work on those for 12-18 months
4. Treat the program like a marketing effort
5. Phish frequently, once a month minimum

Source: KnowBe4

Routine Testing

Testing employees' ability to recognize phishing attacks has two benefits:
1) Businesses can see which employees fall for these types of attacks. Once you know who is susceptible to social attacks, you can offer additional training and resources to those employees.
2) Routine testing creates top-of-mind awareness of social attacks and IT security for your employees.