

SecurityAwarenessNews

the security awareness newsletter for security aware people

SCARE TACTICS: HOW CON ARTISTS USE FEAR FOR PROFIT



SCAREWARE BASICS



Imagine you are browsing the internet, and a bright box pops up on your screen. It states: "Warning! Your computer is infected with a dangerous virus!" It tells you that your data is being actively stolen and urges you to download a fix for the device immediately.

This is a classic example of scareware.

Scareware is a type of scam that uses fake warnings to trick people into thinking a device is broken or infected.

Con artists use scareware to trigger panic and worry. When people feel scared, they might react quickly without thinking things through. And if they fall for the scam, this is what can happen:

THEY DOWNLOAD MALWARE

Short for malicious software, malware is dangerous code designed to damage your device, spy on your keystrokes, or steal your private passwords.

THEY GET SCAMMED OUT OF MONEY

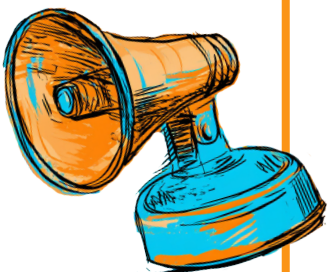
Scammers often try to sell fake security software. The victim ends up paying real money to fix a problem that never existed in the first place.

THEIR PRIVATE INFORMATION IS STOLEN

A scareware pop-up could send the victim to a malicious website that prompts them to enter personal information, such as passwords, home addresses, or credit card numbers.

HOW TO PROTECT YOURSELF

Scareware only works if you let fear take over. Real antivirus programs run quietly in the background and will not show dramatic, flashing ads on a website. If you see a random pop-up, do not click anywhere on it. Close your browser tab immediately. If you encounter any unusual warnings while working, report them right away.



CRITICAL THINKING: YOUR TOP DEFENSE

Cybercriminals know that human beings are wired to react to strong emotions. That's why they use tactics of emotional manipulation called social engineering. **Social engineering is the act of deceiving people into giving up confidential information or breaking normal security rules.**

Social engineers want to use your emotions against you, and fear is one of their favorite weapons. Scammers exploit this by creating a false sense of urgency and using threatening language that can cause someone to take a quick action.

Here are a couple of examples of how this works:

THE LOCKED ACCOUNT TRICK

You receive an urgent email claiming your bank account has been locked due to suspicious activity. The attacker wants you to panic and open a malicious link.

THE AUTHORITY SCARE

A caller pretends to be a debt collector and claims you owe money for an outstanding debt. They threaten you with legal action if you don't pay immediately.

ACTIVATE YOUR CRITICAL THINKING

Your best defense against these scare tactics is to use critical thinking and practice security awareness by:

- **Staying Alert:** Scams work best when people are busy or stressed, so don't let your guard down.
- **Slowing Down:** Always remember that attackers want you to take immediate action before logic sets in.
- **Remaining Skeptical:** If you receive a random request for money or private information, approach it as if it's a scam.

Never let an emotional message push you into a rushed mistake. When in doubt, stop communication and verify the request through a trusted channel.





SPEAR PHISHING: THE ADVANCED ATTACK

You likely already know about phishing, a scam in which attackers send malicious emails to hundreds or even thousands of people at once. The goal is to cast a wide net and hope that at least one person makes a mistake.

However, there is a much more dangerous version called spear phishing. **Spear phishing is a highly targeted attack directed at a specific person or organization.** Instead of a generic message, the scammer uses personal details to make the message look completely real.

To pull off this type of attack, criminals often follow a common process that goes like this:

First, they do their research by reviewing public websites and social media to gather as much information as possible. They want to discover where someone works, what their job title is, and anything else they can find.

Next, they impersonate a trusted source.

This can involve creating fake email addresses that look identical to someone the target knows or a service they use.

Finally, they'll craft a custom message that reads naturally and sounds believable.

Since the message appears to come from a familiar source, the recipient is much more likely to trust it.

When successful, these attacks can scam people and organizations out of large sums of money or lead to data breaches involving highly confidential information.

To avoid falling for these targeted attacks, always closely review the sender's full email address and check for anything odd, like misplaced characters or letters. Be suspicious of any unusual or urgent requests, even if they appear to come from a manager or co-worker. And make sure you always follow your organization's policies, which are designed to protect data, devices, and people.