SecurityAwarenessNews

the security awareness newsletter for security aware people

The Foundations of Security Awareness

Awareness in Action

Top 5 Security Fundamentals

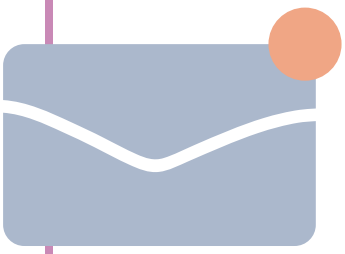
Fantastic Scams and How to Avoid Them

Awareness in Action

Put yourself in the following situation.

It's a normal work day, and you're managing your inbox. You notice an email from human resources about an employee performance assessment. The message doesn't address you by name but claims that your annual performance review is complete.

The email urges you to click the provided link immediately to view your report since this information is used for salary increases and promotions.



Now, this could be a legitimate scenario. Most organizations conduct performance reviews semi-regularly. Security awareness, however, would implore you to question whether this is a scam. Why? Here are a few reasons:

- **Attackers often impersonate human resources:** It's one of the most common scams around
- **No name; no legitimacy:** If this were communication from HR, the email would likely address you by name
- **A sense of urgency:** Scammers always want their targets to believe if they don't act immediately, something bad will happen

There's also missing context in this scenario that would provide insight. For example, does the email come from an actual person at your organization, or is it generic? Does the link appear trustworthy when you hover your mouse over it, or does it lead somewhere strange? Were you given prior information about a performance review?

Asking those types of questions is an example of security awareness in action. To refresh what that means, security awareness refers to someone remaining knowledgeable of the various threats to data, systems, and people. It's a proactive approach that avoids assumptions and instead searches for any indicators of potential scams.

By taking this approach, you can successfully navigate scenarios like the example we just covered. So stay alert, stay informed, and be sure to report anything suspicious immediately per your organization's policies.

Top 5 Security Fundamentals

Teachers, athletes, artists, and others often refer to mastering the fundamentals of their craft. It's a process rooted in gaining a conceptual understanding of the essential skills and principles necessary for continuous improvement.

The craft of security awareness is no different. While we could list a dozen principles relevant to that concept, these five stand out as the fundamentals.

One: Strong Passwords Are Vital to Security

Many online accounts provide access to confidential information. It is, therefore, imperative that those accounts are never compromised, which means ensuring they're protected with strong passwords. As a refresher, a strong password is long, unique, and adheres to organizational requirements.

Two: Social Engineers Hack People, Not Technology

Social engineering is the use of deception to con people into making costly mistakes. Social engineers create fake yet believable scenarios designed to steal money or information. You can avoid falling for their scams by thinking critically and never making assumptions.

Three: Phishing Attacks Remain the Top Threat

Phishing scams attempt to lure people into doing something they shouldn't, such as opening a malicious link or attachment. These attacks are the top cause of malware (malicious software) infections, data theft, and other harmful consequences. Avoid them by slowing down and thinking before clicking.

Four: Physical Security Is as Important as Cybersecurity

Understandably, security efforts tend to focus on digital threats, such as phishing emails and malware. However, physical security deserves just as much consideration. This includes simple actions, like locking devices when not in use and properly storing anything confidential.

Five: Following Policy Helps Protect Everyone

Policies are designed to maintain the security of everyone associated with an organization. They're the guidelines that exist to minimize mistakes and mitigate threats targeting systems, data, and people. Always following policies represents one of the easiest actions any individual can take.

Fantastic Scams
and How to Avoid Them

Most people believe they'll never fall for a scam, but the truth is that some scams are fantastically clever. Let's review a few that anyone might encounter.

This common phishing attack often occurs via email or a phone call. It typically claims that your account has been suspended due to fraudulent activity. You must update your login credentials, or the account will be closed permanently.

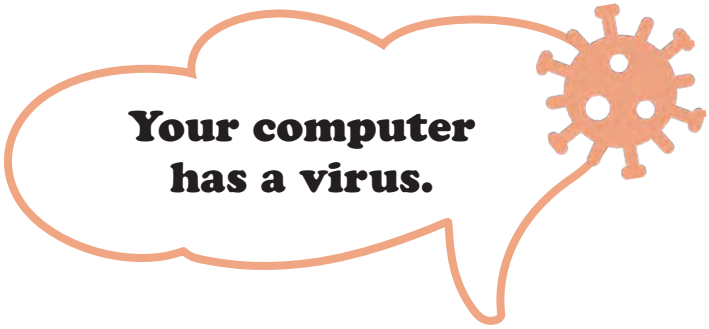
Don't fall for it. Most organizations or institutions won't ask you to confirm highly confidential information via email or over the phone.

This common extortion scam starts with an email with a threatening subject line like, "I saw what you did!" The messenger claims they hacked your computer and recorded you via your webcam. They then threaten to send the video to your contacts unless you immediately pay the scammer.

Don't fall for it. This one can make people feel uncomfortable, but that's the whole point. Extortion attempts should always be ignored.

Imagine receiving a phone call from someone who knows your name, your address, and claims that you owe a debt. Failure to pay that debt will result in legal action and you will need to appear in court.

Don't fall for it. In most cases, debt collectors are lawfully forbidden to pressure people into payment and must provide several details regarding a debt. Scammers won't have those details.



This scam occurs when you're browsing the internet and encounter a pop-up that states your device has a virus. Clicking on it will take you to a payment form for a service or application that will "fix" the nonexistent virus.

Don't fall for it. Avoid clicking on pop-ups when browsing the internet and never install random software.