SecurityAwarenessNews

the security awareness newsletter for security aware people

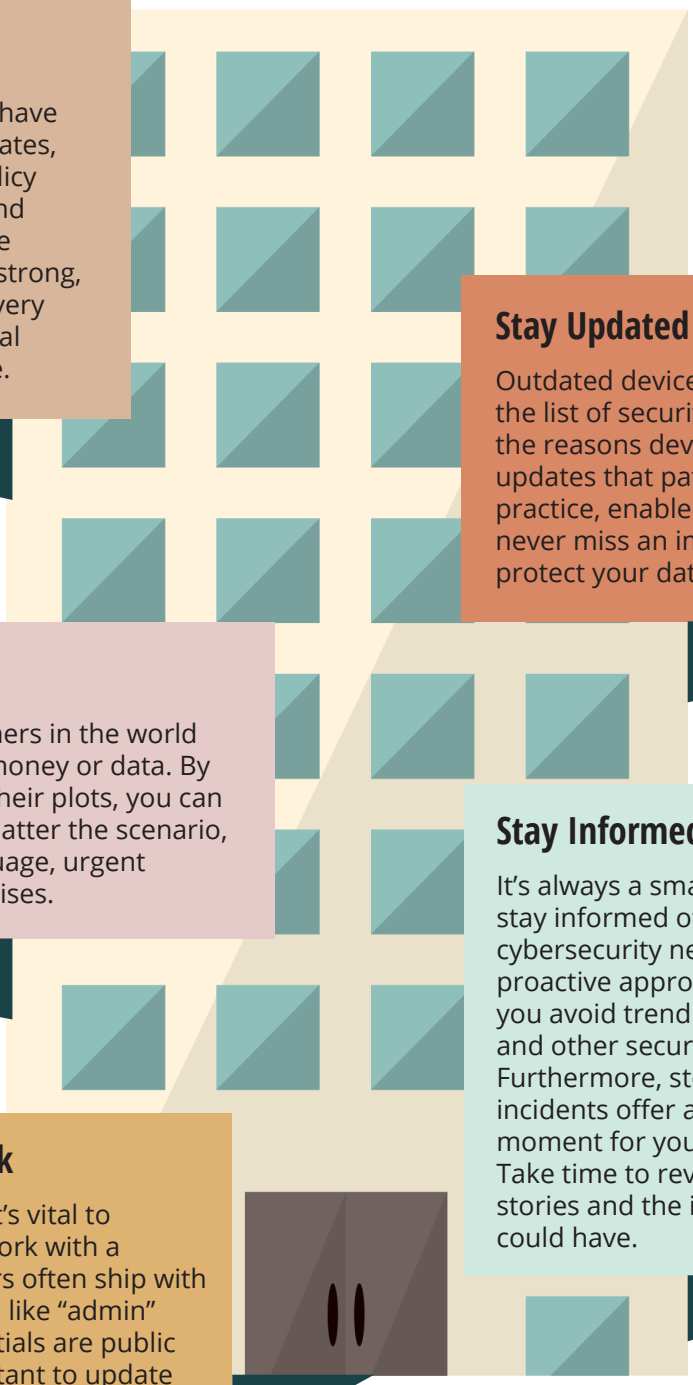
The Personal Side of Security

Taking Security Awareness Home
Navigating the Privacy Paradox
Getting Personal with Passwords

Taking Security Awareness Home

Given the landscape of ongoing security threats, most organizations require team members to take regular awareness training. It's also vital to remember security threats extend far beyond the workplace. Scammers don't mind getting personal. They'll target anyone anywhere, not just organizations.

That's why it's a good idea to apply awareness training concepts to your personal life. Protect yourself. Protect the people you care about. Here's how:



Develop Household Security Policies

Whether you live alone, have kids, or live with roommates, a household security policy serves to protect data and devices. It should include simple things like using strong, unique passwords for every account and setting social media profiles to private.

Stay Updated

Outdated devices and software often top the list of security concerns. It's one of the reasons developers routinely push updates that patch vulnerabilities. As a best practice, enable automatic updates so you never miss an important fix that could help protect your data.

Learn the Warning Signs

There is no shortage of scammers in the world who would love to steal your money or data. By learning the warning signs of their plots, you can avoid becoming a victim. No matter the scenario, stay alert for threatening language, urgent requests, and unrealistic promises.

Stay Informed

It's always a smart idea to stay informed of current cybersecurity news. This proactive approach can help you avoid trending scams and other security threats. Furthermore, stories of security incidents offer a great teaching moment for your household. Take time to review those stories and the impact they could have.

Protect Your Network

Like an online account, it's vital to protect your home network with a strong password. Routers often ship with default login credentials, like "admin" or similar. Those credentials are public knowledge, so it's important to update them to something strong immediately.

Navigating the Privacy Paradox

The concept of personal privacy is at odds with the wealth of convenience the internet provides. This conundrum has given rise to what's known as the privacy paradox. It refers to people who, despite concerns about their privacy, disclose personal information so they can access free online services.

Nothing, of course, is ever actually free. Those services are usually provided in exchange for your browsing habits, age, location, and other personal details, which will be used for marketing purposes.

The question then becomes, what actions can anyone take to balance their privacy with online convenience? The answer isn't easy, but there are at least a few ways to control your privacy.

Review Permissions

Whenever you install mobile apps, take a minute to review permissions. Decline any that aren't necessary for the app to function. For example, a mobile game shouldn't need access to your contacts or messages.

Opt Out

You've probably noticed that many websites ask you to accept or reject cookies. These cookies are how sites store various settings for the next time the user visits. Feel free to reject them for any sites you don't regularly frequent.

Go Incognito

Most modern web browsers offer an incognito or private browsing mode. It lets you use the internet without the browser tracking your history. This function can help you avoid unwanted advertisements and data collection.

Install Privacy Extensions

There are several browser extensions geared towards privacy that prevent websites from tracking or monitoring your web activity. They also eliminate pop-ups, which can help you avoid potentially malicious advertisements.

While these privacy measures won't fully remove the concerns of data collection, they can help manage how your personal information is used. Like all things related to personal security, being proactive is the key.

Getting Personal With Passwords

At work, it's your responsibility to ensure your passwords adhere to organizational policies. At home, password maintenance becomes a personal matter. Unless you have a dedicated IT department, no one is going to tell you how to create your login credentials.

Even so, work and personal passwords do have something in common: Weak ones are major security risks. With that key fact in mind, let's review ways to ensure your passwords meet modern standards.

Be Unique

The world would be a boring place if every person were exactly the same. Don't make online security boring (and vulnerable). Instead, ensure every account gets a unique password. If you reuse a password and it gets stolen, someone could use it to gain access to any account with that same password.

Phrase it Correctly

Passwords should be long and never used twice. Unfortunately, that also makes them difficult to remember. One solution to this is stringing words together to form a passphrase, such as an obscure quote from a book. The idea is to create passphrases that are easy to remember but hard to guess.

Use a Password Manager

Forget memory problems. Why not use one password to rule them all? That's the idea behind a password manager. It's software that creates, stores, and syncs every login credential across multiple devices. You only have to remember one (very strong) password to unlock software and access logins.

Add More Layers

Imagine if a cybercriminal managed to steal one of your passwords. What's to stop them from taking control of the associated account? Answer: Multi-factor authentication. It's a great feature that adds an extra layer of security by requiring more than one code to access an account. Enable it wherever possible.