SecurityAwarenessNews
the security awareness newsletter for security aware people

# Personal, Family, and Home Security

## Taking Security Personally

## Security Without Paranoia

## Security Tips for Parents

# Taking Security Personally

It goes without saying that no one wants to make the news for suffering a data breach or any other security incident. That's why we constantly push security awareness as a default responsibility required of every member within our organization.

We also want to stress that almost every security awareness issue we cover at work can and should be applied to your personal life. We believe that the key to a better world (in terms of security) is education and building a culture that prioritizes awareness 24/7. With that in mind, let's review a few fundamentals of security awareness, and how you can take them personally.

## Passwords

Never use the same one twice. Don't write them down. Never share them. Substitute traditional passwords with passphrases such as "welcometothepartypal!" and consider getting a password manager–software that creates, stores, and syncs all of your logins across multiple devices.

## Phishing

Still the most common way cybercriminals infiltrate organizations; stay alert for phishing attacks at home. Look for red flags such as bad spelling and grammar, unrealistic promises, urgent or threatening language, and unexpected links or attachments. Remain skeptical of any request for personal information or money.

## Software Updates

One of the easiest ways to prevent malware infections or data leaks is by keeping your devices and software up to date. Many software updates patch vulnerabilities that cybercriminals use to their advantage. Stay current by enabling automatic updates wherever possible.

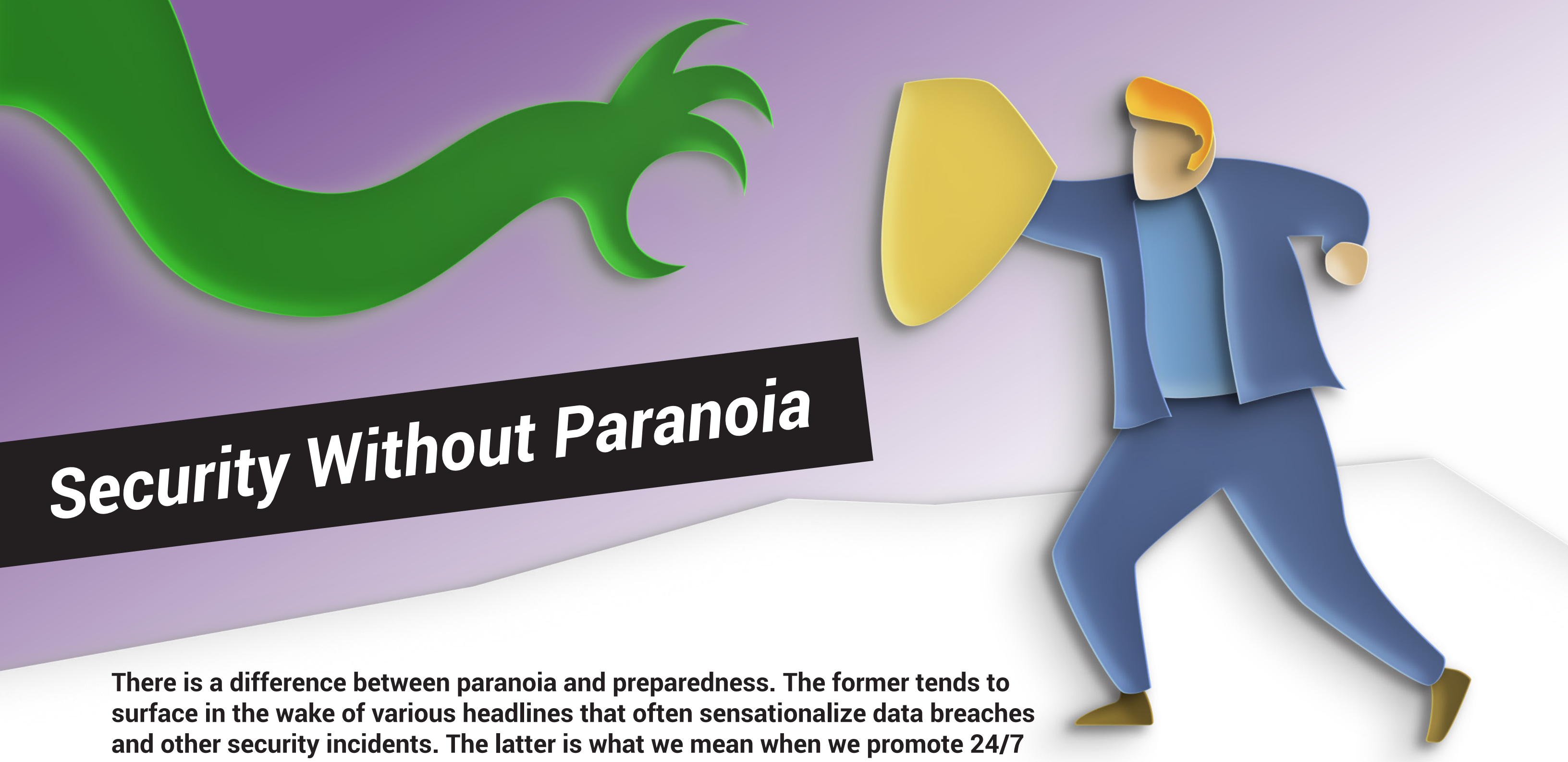
## Social Media

Did you know that scammers surf social media and other public forums to gather intelligence and build profiles of their victims? The more you share publicly, the bigger the target you become. Double check your privacy settings and only "friend" people you know.

## Physical Security

Cyber attacks get all the headlines, but don't overlook the importance of physical security. Shred sensitive documents when no longer needed. Keep an eye on your belongings when in public areas. And ensure no one can see your screen or hear your phone calls.

**These are just some of the security measures you should take home with you. We encourage you to set up your own security policies suitable for your household. Here at work, always follow our organization's policies, and if you have any questions, please ask!**



# Security Without Paranoia

**There is a difference between paranoia and preparedness. The former tends to surface in the wake of various headlines that often sensationalize data breaches and other security incidents. The latter is what we mean when we promote 24/7 security awareness–a simple understanding that scammers are everywhere and target everyone. Here's how you can prepare for security threats without paranoia:**

**Paranoia:** *Never using a public WiFi network.*

**Preparedness:** *Always using a Virtual Private Network (VPN).*

**VPNs encrypt your internet connection making it difficult for cybercriminals to intercept and steal your data. Never connect to public WiFi without a VPN, and even then, avoid accessing highly sensitive information.**

**Paranoia:** *Never sharing any photos or updates on social media.*

**Preparedness:** *Using the security settings on your social media accounts.*

**As a general rule, it's best to set your social media accounts to fully private and ensure that your friends and followers are people you know and trust. It's also smart to occasionally audit your list of friends and remove anyone you rarely connect with in real life.**

**Paranoia:** *Refusing to install apps on your smart device.*

**Preparedness:** *Researching and downloading apps from trusted sources.*

**Malicious apps are an ongoing security issue with app stores. Do your research before installing anything and carefully review permissions and security settings after installing. Routinely uninstall apps you no longer use.**

**Paranoia:** *Frequently updating every single password.*

**Preparedness:** *Utilizing multi-factor authentication (MFA).*

**MFA adds an additional layer of security by requiring a second code to unlock an account. This way, if a major data breach leaks your login credentials, it will still be difficult for an unauthorized person to gain access.**

## Is covering a webcam paranoia or preparedness?

It's a little bit of both. We know for a fact that cybercriminals can hack webcams. So, it's not a terrible idea to cover them. But truthfully, it's not the webcam that gets hacked, it's the human. In most cases, the victim clicked on something they shouldn't have, which gave the attacker access to the victim's camera (and microphone and likely the entire computer). Unless you're a high-profile individual–such as a celebrity or government official–it's unlikely you'll be targeted (at least when you're in the comfort of your own home).

So don't be paranoid. Instead, be proactive! Think before you click. Keep your apps and devices up to date. Install antivirus software on every device. And if you choose to cover your webcam, don't use tape. Buy a cover that fits your device and won't leave a sticky residue.

# Security Tips for Parents

**Parenting is hard enough before even considering the challenges of online security. What follows are five tips to help you meet those challenges. Obviously, every household has different needs, so view these as a generic starting point, and make adjustments as necessary!**

### *Establish a culture of trust.*

Create a safe space where honesty won't be punished and where kids feel comfortable sharing their experiences. If they witness cyberbullying or inappropriate behavior online, or accidentally share something they shouldn't have, we want to make sure they'll speak up before it's too late. Establishing a culture of trust is the best way to gain and maintain a healthy digital presence in your household, and it needs to start at a young age.

### *Explain the risks of social media and online behavior.*

Just like in real life, children should be taught that their online actions come with consequences. Posting harmful content on social media could prevent them from getting jobs or scholarships. Sharing too many personal details could lead to identity theft. Being a troll or a cyberbully might cause great emotional distress for someone else. It's imperative that our young digital citizens understand how powerful the internet is, and that misusing that power will carry repercussions.

### *Utilize parental control solutions.*

While it's important to respect the privacy of our children, it's also important to do what's best for their safety. Parental control software allows you to monitor internet activity, set time limits, manage contacts and messaging apps, and a bevy of other options that can be customized to fit your household's needs. Additionally, consider installing antivirus software on every device that allows it.

### *Set up separate user accounts.*

Creating different user accounts allows you to control who gets access to what on shared devices. This is particularly important on any computers that are used by adults and young people because it prevents children from accessing games, files, or accounts that are reserved for mature individuals. This separation also allows you to provide access to certain accounts on a case-by-case basis (such as when multiple age groups share one device).

### *Demonstrate the value of screens off.*

Between work, schoolwork, entertainment, and all of the other built-in reasons to use smart devices, we are accustomed to spending most of the day staring at screens. Unfortunately, excessive screen time presents health risks and can deteriorate relationships. Improve the health of your household by dedicating blocks of time where screens are not allowed for any reason. And this goes for parents too, who must lead by example and highlight the importance of screen-free family time.