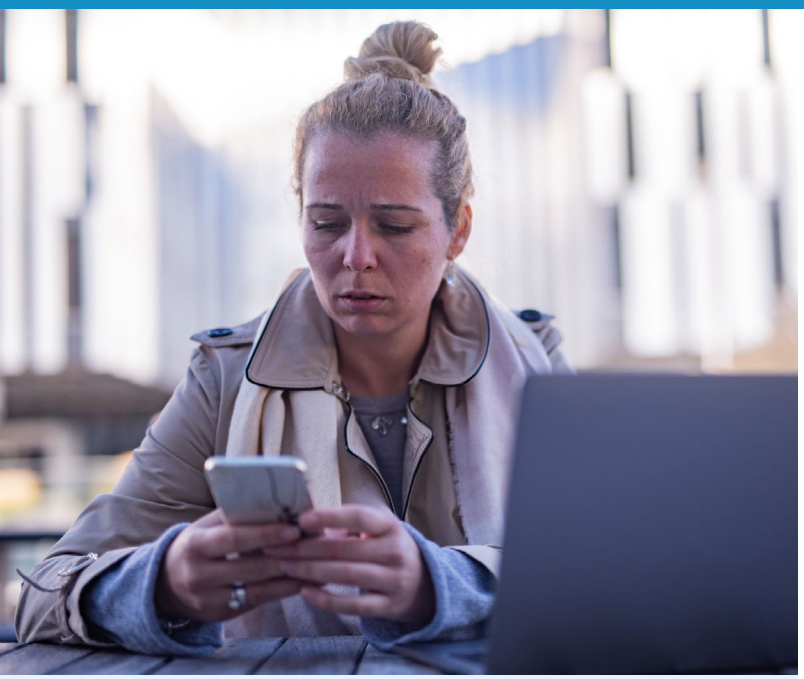

"As cyber threats evolve, we need to evolve as well."
- FBI Director Christopher A. Wray

Cybercrimes Diminish Victims' Wellbeing

The chance of becoming a cybercrime victim is increasing daily as bad actors around the world expand the variety, scope and sophistication of their attacks.

Cybercrime seems impersonal because it is anonymous and depends on technology to commit. But it has intensely personal consequences for individuals who are targeted. Victims often experience a sense of loss that impacts their mental and physical health.

Mental health symptoms may range from low mood and mild anxiety to severe depression and other forms of psychological distress. Physical complaints may include sleep disruption, fatigue, loss of appetite, gastrointestinal upset, headache, muscle tightness and high blood pressure.

Crime victims, in general, are at risk for the development of post-traumatic stress disorders. With cybercrime, the uncertainty of not knowing the extent of a breach or the potential for future attacks can heighten anxiety, affect concentration and make it hard to do routine tasks. Adults, teenagers and children who are subjected to online bullying, cyberstalking or harassment may withdraw, experience flashbacks, have nightmares and/or become hypervigilant.

Cybercrime victims may lose confidence in their own judgment and institutions they trust to protect their identity, sensitive personal information, financial assets, business interests and loved ones. This can lead to social isolation and depression. When a person falls for a romantic or financial scam, they may feel deeply upset, sad or hopeless. Victims who are self-incriminating or ashamed tend to be less inclined to admit what happened and more likely to adopt unhealthy coping strategies such as substance use.

Human Factors

Cybercrime cannot be prevented with technological countermeasures alone, partly because it co-exists with legal business practices such as tracking people's online searches to promote products and services. Individual personality traits, online habits and a person's degree of familiarity with technology also influence vulnerability.

For example, a potential victim may not understand the magnitude of their exposure risk, be insufficiently suspicious or just not pay close enough attention to stop a fraudulent process. (Refer to *Current Psychiatry Results*.) Psychologists estimate 5 to 10 percent of Americans meet criteria for social media addiction, which may increase their exposure to cyberattacks. Studies show that constant social media engagement triggers the brain's reward center and releases a dopamine rush similar to that experienced by gamblers and some illicit drug users.

While anyone with a credit card or digital records can become the passive victim of a cybercrime committed against a business entity, a survey of 11,780 people found that targeted individuals are more likely to score high on measures of impulsivity, urgency, sensation-seeking and addictive tendencies. (Refer to Journal of Financial Crime.) Age is also a factor. Older people are more likely to be victims of financial scams, while younger people tend to be victimized socially.

What Can You Do?

Feelings of betrayal, helplessness and loss can be difficult to overcome. It's important for cybercrime victims to seek support from friends and family members, and to consult with medical and behavioral health professionals when they are experiencing symptoms. Taking control by reporting an incident to law enforcement and strengthening cybersecurity can also help mitigate personal impacts.

Here are some preventive recommendations:

1. Keep track of evolving cybersecurity threats and best practices to prevent cyberattacks.
2. Use updated antivirus software, firewalls, dual authentication and other security tools at work and at home.
3. Make sure you have a secure internet connection, especially in public places.
4. Choose strong passwords and change them frequently. Don't share passwords with others, save them in a browser or use the same one for multiple accounts.
5. Be mindful. Avoid clicking on pop-ups, suspicious links, downloading files from untrustworthy sources and oversharing personal information on social media.
6. Review your social media profiles and remove personal/private information that may increase your susceptibility.
7. If you use dating sites and similar online forums, do not send money or give personal information to someone you don't know – even if you *think* they are trustworthy.
8. Help protect children, teenagers and vulnerable adults who do not fully comprehend cybersecurity threats.

The cybercrime landscape is constantly evolving. What you see and read is not necessarily true. Cybercriminals often adapt their tactics to exploit new vulnerabilities and take advantage of popular culture trends. It's crucial to be well informed about cybersecurity best practices and regularly update defenses.

Employees Susceptible to Digital Alert Fatigue

Cyberattack threats in the workplace contribute to alert fatigue and increase risk for employee burnout, Security magazine reports.

Research shows that digital overload and multiple communication channels in the workplace reduce productivity and lead to a decline in engagement with cybersecurity training. As a result, employees are more vulnerable to cyber threats, such as phishing emails, and more likely to skip using multi-factor authentication and other protective measures.

According to survey results released by CybSafe:

- *70 percent of U.S. office employees surveyed said they feel overwhelmed with the amount of information and digital communication they receive at work.*
- *54 percent acknowledge that they ignore cybersecurity alerts and warnings due to information overload from digital communication.*
- *47 percent of respondents said information overload impacts their ability to identify threats such as suspicious emails.*

Employers are encouraged to find ways to make cybersecurity training more engaging and create work-related digital experiences that are easy to navigate and as seamless as possible.