DigiKnow
CYBER SECURITY DEPENDS ON YOU

Cyber Threats and Trends for 2020

Windows 7 Reaches End of Life

Microsoft made a commitment to provide 10 years of product support for Windows 7 at its release, October 22, 2009. Microsoft discontinued Windows 7 support effective January 14, 2020. ***Technical assistance and software updates from Windows Update that help protect your PC are no longer available***. The State Chief Security Office and Microsoft strongly recommend that you move to Windows 10 now. There is no more service, security protection and support for Windows 7 from Microsoft. State of Delaware systems still using windows 7 will begin to lose critical services like Internet browsing access. Contact your local IT Support team if you are still running this unsupported Operating System.

— Solomon Adote, Chief Security Officer

Beware of Online Dating Scams

AARP says, if you're looking for love online, make sure to keep your wallet — if not your heart — under lock and key. Fraud cases are climbing as the numbers of dating sites and apps and users grow.

Today there are an estimated 25,000 romance scammers online worldwide, according to one cybersecurity expert. Between 5 and 25 percent of online daters could be fakes or scammers, says another.

Dating scams come in many forms, but here is a list of major red flags to avoid:

- The person seems to develop very strong feelings for you very quickly; they may say they've fallen in love with you or can't live without you within just a few days or weeks of online communication.
- Their dating profile only has professional photos and/or the person is extremely attractive and often quite a bit younger than yourself.
- There are many typos and grammatical mistakes .
- They may tell you they've just experienced a horrible tragedy—a layoff, a dramatic death in the family.

What's HOT In Cyber Threats?

CSO Online took a look at greatest challenges facing Security professionals. Here are some of their findings:

Credential stuffing - Every year it seems that there's a constant *drip-drip* of major hacks at big companies that result in millions of username/password pairs being compromised. The real-world consequences of these attacks are what's known as *credential stuffing,* when an attacker uses long lists of stolen login credentials in large-scale automated attempts to log in to various websites. The attackers rely on the fact that many of us use the same username and password on multiple sites. Thanks to the attacks' automated nature, even if only a small percentage of the stolen login credentials are a positive match, it can still be worth the attackers' while.

Banking trojans—A slew of trojans have hit the scene that focus specifically on gaining access to user accounts at financial institutions. These trojans spread in the usual way—phishing sites, hijacked emails, and the like—but once installed become laser-focused on user interaction with banking sites, attempting to harvest login information via keylogging and other spyware techniques, which is then reported back to the criminal controllers.

The Internet of Things (IoT)—This an umbrella term that covers a disparate host of gadgets smaller and simpler than a computer, connected to a wireless network, and deployed for specific purposes. These gadgets range from industrial sensors to smart home thermostats. Unfortunately, IoT devices are often non-standardized, lack built-in security, are difficult to administer remotely, and have just enough inherent functionality to be hacked, allowing bad actors into an otherwise secure network.

Phishing—The art of tricking users into giving up login information—certainly isn't novel anymore, but it's still a favorite of attackers. "Increasingly, employees are being subjected to targeted phishing attacks directly in their browser with highly legitimate looking sites, ads, search results, pop-ups, social media posts, chat apps, instant messages, as well as rogue browser extensions and free web apps," says Atif Mushtaq, CEO and founder of *SlashNext.* Be careful where you click!

Questions, comments or topic suggestions? Email us at eSecurity@delaware.gov