DELL Technologies

Cyber Safety Cheat Sheet

In our increasingly virtual world, cybercrime is – not surprisingly – growing at an alarming rate. In fact, **cybercrime generated roughly $6 trillion in 2021**, making it the third largest economy in the world after the U.S. and China!* Attackers are getting smarter and more sophisticated by the day, but it's easy to be safe online when you're aware of the latest threats and have protective measures in place. **Here are some of the threats Dell's cybersecurity experts are working hard to prevent and tips on how to keep your workplace and household secure.**

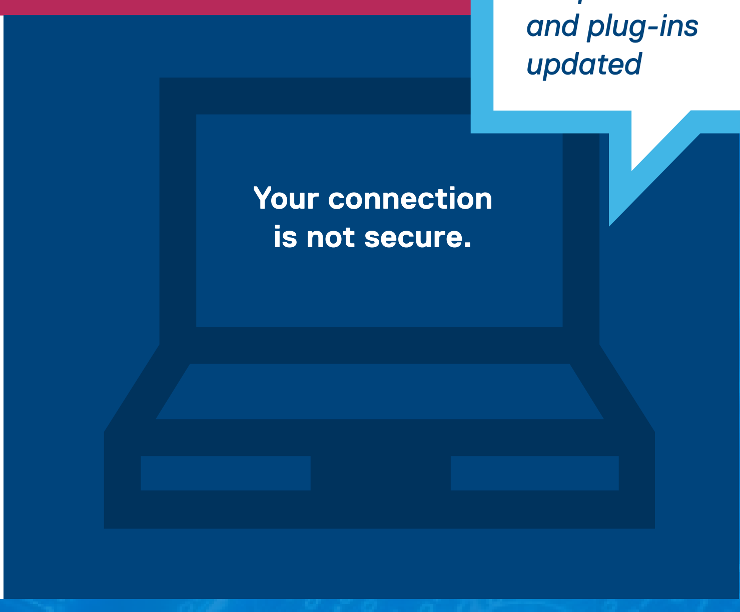
Drive-by Compromise

Malicious parties get access to your system when you stumble across an unsecure or compromised website.

How to spot it:

New files or network connections on your system that you did not add

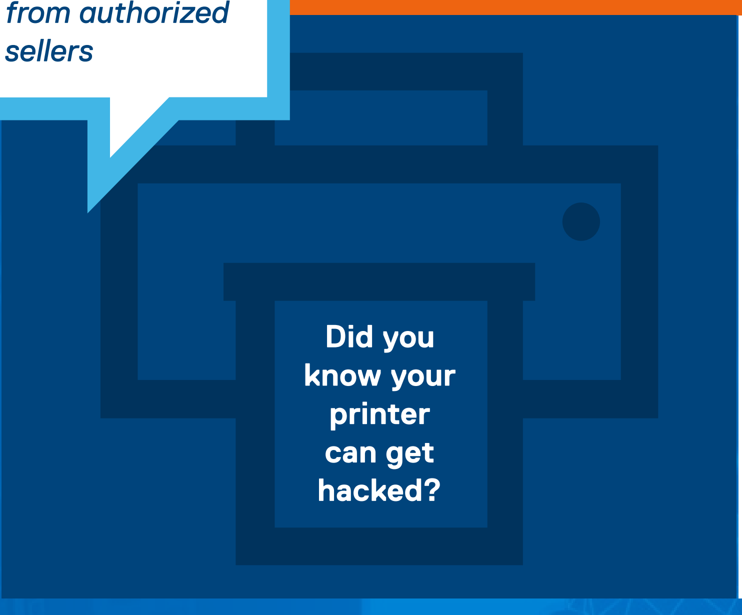
Unsolicited requests for configuration information



TIP: *Keep browsers and plug-ins updated*

Unsafe Hardware

TIP: *Make purchases from authorized sellers*



Threat actors embed vulnerabilities directly into hardware and accessories.

How to spot it:

Too-good-to-be-true deals

Social Engineering

Scammer manipulates people by pretending to be a legal entity or other authoritative body to steal their sensitive **personal or financial information** (a.k.a. "phishing"). The malicious code is sent via links or attachments to emails, direct messages and texts.

How to spot it:

Unsolicited emails or texts asking for personal information with directions to open links and attachments

Odd sender email address, phrasing, spelling

TIP: *Government agencies (IRS, etc.) will reach out via USPS first*

USB Malware Attack

TIP: *Be wary of unknown USB drives, even if shared by friends*

Criminal uses removable storage devices, like USB drives, portable hard drives, smartphones, music players, SD cards, and optical media (CDs, DVDs, BluRay), to infect a computer or network.

How to spot it:

Unexpected access to files or newly created files on the device

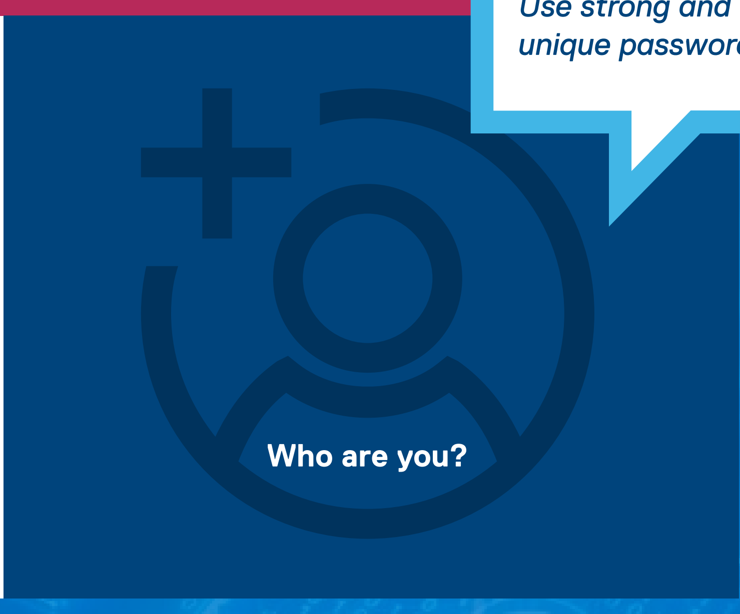
Trusted Relationship

A hacker breaches a trusted third party, like a doctor's office, and uses their reputation to exploit patients.

How to spot it:

Unusual logon behavior

TIP: *Use strong and unique passwords*



How to stay cybersafe:

DOs

Use multi-factor authentication and strong, unique passwords across all of your accounts.

Any device connected to the internet is open to attack. Keep software up-to-date.

Be alert and skeptical. Learn to recognize scammer tactics.

Be vocal. Report attacks to IT and notify coworkers, family, and friends.

DON'Ts

Don't get lazy. Follow all security protocols consistently.

Don't click on any links embedded in unsolicited emails or direct messages.

Don't ignore browser warnings, e.g., "Your Connection is Not Secure" or "Your connection is not private".

TIP: *For more information, visit:* Dell.com/Endpoint-Security

DELL Technologies

*Cybersecurity Ventures: 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics