CYBERSECURITY TIPS OVERVIEW

(773) 305-3535 | SHARTEGA.COM | 1350 E TOUHY AVE SUITE 350E, DES PLAINES, IL 60018

Keep your software up-to-date

Software companies typically provide software updates for 3 reasons: to add new features, fix known bugs, and upgrade security.

Always update to the latest version of your software to protect yourself from new or existing security vulnerabilities.

Keep your hardware up-to-date

Outdated computer hardware may not support the most recent software security upgrades.

Additionally, old hardware makes it slower to respond to cyber attacks if they happen. Your IT provider should have information about the age of your hardware.

Avoid opening suspicious emails

If an email looks suspicious, don't open it because it might be a phishing scam.

Someone might be impersonating someone you know in your organization to gain access to your personal information. Sometimes the emails can include attachments or links that can infect your devices.

Use anti-virus and anti-malware

As long as you're connected to the web, it's impossible to have complete and total protection from malware. However, you can significantly reduce your vulnerability by ensuring you have an anti-virus and at least one anti-malware installed on your computers.

Use a secure file sharing solution

The files you share are only as secure as the tools you use to share them with. Adopt a secure file sharing solution to encrypt your files while they're in transit and at rest to prevent unauthorized access and keep your files safe.

Use a password manager

Get your business a subscription to a password manager like LastPass.

Password managers are essential for keeping your many account passwords secure and can also be used to generate new, strong passwords.

Enable multi-factor authentication

Many platforms now allow you to enable multi-factor authentication (MFA) to keep your accounts more secure.

It's another layer of protection that helps verify that it's actually you who is accessing your account and not someone who's unauthorized. Enable this security feature when you can.

Train your employees on cybersecurity

The key to making cybersecurity work is to make sure your employees are well trained, in sync, and consistently exercising security best practices. One mistake from an improperly trained employee can cause an entire security system to crumble.

Double check for HTTPS on websites

When you're on a website that isn't using HTTPS, there's no guarantee that the transfer of information between you and the site's server is secure.

Look for HTTPS at the beginning of a website's URL or look for a small padlock symbol in the address bar.

Back up important data

Important data can be lost as a result of a security breach. To ensure that you're prepared to restore data once it's lost, you should frequently back up your important information with a cloud backup solution like Acronis Cyber Protect, or to a local storage device.

HOW TO SPOT A PHISHING EMAIL

Can You Spot The Errors in This Phishing Email?

1 Payment Declined -- Update Required Immediately!

2 From: **ApplePay Support** <customer_support_ref_@apple.com>

3 Dear Apple User,

4 It has come to our attention that you're recent payment was declined. An update is required immediately..

To make this change, visit the support section at the link below.

5 https://www.applepay.com/subscriptions/payment-update

http://944.535.32/index/apple.html

6 **If you do not update your payment information in the next 24 hours, your account will be deactivated.**

7 Regards
ApplePay Support

—

8 Copyright © 2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001

9 ZIP apple-invoice.zip Download

1. Sense of urgency
   Fear tactics
2. Imitating known brand
   Fake email address
3. Impersonal
4. Urgency
   Punctuation and grammar mistakes
5. Rollover shows malicious link
6. Scare tactics
7. Impersonal
   Not real customer service
8. Copyright date is incorrect
   Location is incorrect
9. Zip file

What Is A **Clean Desk Policy?**

Clean desk policies ensure desks are left tidy, organized and secure when employees leave their workspace for the day. Offices implement these policies in an effort to increase security, cleanliness, professionalism, and efficiency.

Keeps the workspace free of clutter

Computers locked and USB drives stored away

Don't write down passwords on paper

Sensitive documents kept out of view or shredded