Cybersecurity : Safe Browsing for Employees

DIGITAL TECH
PARTNERS

www.digitaltechpartners.com

Safe Browsing Practices

- Don't rely on your browser to protect you from malicious Websites
  - Browsers only warn you about sites
  - They cannot stop you from going there
  - Even with high security settings and anti-virus software, visiting a risky Web site can result in viruses, spyware or worse.
- Keep your browser software up-to-date
  - Do the update immediately upon notification
- Keep operating systems and applications up to date
  - Apply all critical software patches to protect against viruses, spyware, and other malicious software that may infect your system through the browser.

Safe Browsing Practices

- Don’t reuse passwords
  - Using the same password for multiple sites only makes it easier for hackers to compromise your sensitive information
  - Instead, use password managers to track of your different passwords or create unique passwords that only you would know
  - Change your passwords every 90 days

- Read privacy policies
  - Websites’ privacy policies and user agreements provide details as to:
    - How your information is being collected and protected
    - How that site tracks your online activity
  - Websites that don’t provide this information in their policies should generally be avoided

Safe Browsing Practices

- Review web browser default configurations
  - Disable or limit features that make your computer vulnerable
- Be cautious when playing online games or downloading free software
  - Spyware may be bundled with those programs
- Websites use cookies to collect information about you
- If you don’t want to be tracked
  - Configure your browser to delete cookies either periodically or when closing the browser.

Safe Browsing Practices

- Turn on your browser's popup blocker
  - Popup blocking is now a standard browser feature
  - Enable it any time you are surfing the Web
  - If it must be disabled for a specific program, turn it back on as soon as that activity is complete

- Software add-ons that provide functionality to a web browser (e.g., Java, Flash, etc.) may:
  - Introduce vulnerabilities to the computer system
  - Consider enabling add-ons on a case-by-case basis

Safe Browsing Practices

- Run anti-virus software and scan files before downloading
  - Anti-virus software provides protection by scanning for and removing malicious files on your computer
  - Avoid downloading anything until you're confident that it is secure
  - If you suspect that a file may not be legitimate or may be infected
    - Scan it with anti-virus software before downloading

- Use the Secure Sockets Layer (https:) Protocol
  - The "s" in "https" stands for secure, meaning that the Website is employing Secure Sockets Layer (SSL) encryption
  - Check for an "https:" or a padlock icon in your browser's URL bar to verify that a site is secure before entering any personal information

Safe Browsing Practices

- Disable "auto-complete" for forms or "remember your passwords" features
  - Most browsers and websites, generally offer to remember your passwords for future use
  - Scrupulous Web sites can use hidden fields to steal the data from forms.
- Enabling these features makes it easy for Bad Actors to discover if your system is compromised
  - They can hijack your browsing session and steal your information if you stay logged-in to a site
  - If you have these features enabled, disable them and clear your stored passwords.

Safe Browsing Practices

- Regularly monitor your bank statements
  - Review your online bank statements on a DAILY basis
  - Enables you to react quickly when your account has been compromised

- Avoid public or free Wi-Fi
  - Attackers often use wireless sniffers to steal users' information on unprotected networks
  - The best practice to protect yourself from this is to avoid using these networks altogether
  - If you must.. deploy a VPN on your device that will encrypt & protect you on an unsecured network

Cybersecurity Best Practices

General best practices for cybersecurity outlined by the FBI

1. Be skeptical of any last-minute changes in wiring instructions or recipient account information when dealing with Wire Transfers
2. Verify any changes and information via the contact on file
3. Do not contact the vendor through the number provided in the email
4. Ensure the URL in emails is associated with the business it claims to be from
5. Be alert to hyperlinks that may contain misspellings of the actual domain name

Cybersecurity Best Practices

6. Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from

7. Regularly back up data and verify its integrity. Ensure backups are not connected to the computers and networks they are backing up. For example, physically store them offline or in the cloud. If you are infected in ransomware, Backups are may be the best way to recover your critical data

8. Focus on your awareness and training. Since end users are targeted, you should be aware of the threat of ransomware and how it is delivered and trained on information security principles and techniques.

Cybersecurity Best Practices

9. Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered.

10. Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.

11. Implement the least privilege for file, directory, and network share permissions. If a user only needs to read specific files, they should not have write-access to those files, directories, or shares. Configure access controls with least privilege in mind.

Avoiding Social Engineering

1. Verify the identity of those who ask for your sensitive information in person or over the phone before you release it

2. Do not give out system data or sensitive information about other employees, remote network access, organizational practices, or strategies to any unknown individual

3. If you think you are the victim of social engineering, gather as much information as you can, such as the person's name, telephone number, and what they are asking for and report it to your supervisor or information security team.

Turn ON – Multifactor Authentication (MFA)

1. Multi-factor authentication (2FA) solution that allows you to use a second factor that you have or have access to when you log in to your account.
2. That second factor could be an app on a mobile device or receiving a phone call or text message, or even a one-time passcode.
3. Whichever factor is used, the important thing is that should hackers obtain your username and password, they will not have access to your phone or other device and would not be able to complete the login process.

All About MFA
Verifying your identity

Multifactor Authentication is a process where you provide multiple pieces of evidence to verify your identity.

Be AWARE

SENDER

If you don't recognize the email sender, don't open the email

SPELLING

Pay attention to the spelling of email, addresses, subject lines and email content

URGENCY

Be wary of emails that use urgent language and ask you to help out by transferring funds or sharing confidential information

Be AWARE

LINK OR BUTTON

Do not click on links from unsolicited emails

CONFIDENTIAL INFORMATION

Never send confidential information in an email

SECURE WEBSITE

When shopping online, always inspect the address bar and verify that the URL contains "https" or the lock icon

Be AWARE

SOCIAL MEDIA

Do not accept social media followers or friends from accounts that you do not recognize.

If an account that you do not trust follows or friends you, block the account.

For more info, Contact

DIGITAL TECH PARTNERS

Digital Tech Partners, Inc.

63 Tremont Street, Taunton
MA 02780

- jdanahey@digitaltechpartners.com
- www.digitaltechpartners.com
- 774-488-9235
- 339-970-3556 x101

Or Schedule your appointment Here

Follow us on Social Media

Facebook

LinkedIn

YouTube