UPDATED

Cybersecurity Tips for Employees :

Educating Staff on Secure Online & Office Behavior

Contents

((403) 457-1478
https://www.ctechgroup.net

The Need to Educate Employees on Cybersecurity

When developing cybersecurity programs, many businesses focus on protecting their infrastructure perimeter and device endpoints. But it's also important to consider what happens when a threat bypasses perimeter defenses and targets an employee in the form of a malicious email or text.

86% According to a recent PricewaterhouseCoopers survey, 86% of business executives expressed concern about cyber threats and lack of data security.

Stronger cybersecurity has become a global priority as hackers penetrate IT infrastructures with increasing frequency and sophistication. According to the FBI, phishing was the most common type of cybercrime in 2020, with incidents nearly doubling from 114,702 incidents in 2019 to 241,324 incidents in 2020. Not surprisingly, losses from business email compromise (BEC) have skyrocketed over the last year. The FBI's Internet Crime Report shows that in 2020, BEC scammers made over $1.8 billion. Coupled with the Internet of Things (IoT) and the explosive growth of mobile devices, the potential for data leaks is even more significant.

Educating employees on what it takes to protect proprietary documents and data is critical. Any data leaks—whether intentional or unintentional—could potentially damage your bottom line and your industry reputation. It only takes one incident to destroy the goodwill you worked so hard to establish.

Physical Security Precautions

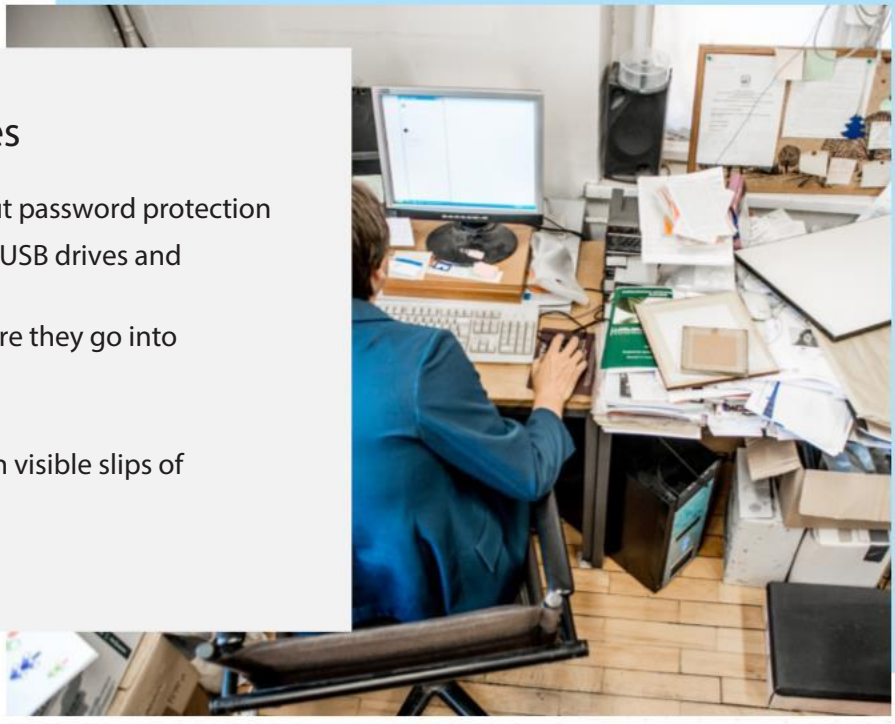
The Importance of Keeping a Clean Desk

It sounds simple, but keeping a clean desk is often overlooked when talking about data security. A messy desk makes it difficult to realize something is missing, such as a folder containing printouts with customer data. A cluttered desk also leads to the discovery of any theft likely being delayed.

Encouraging employees to maintain a neat desk pays off in two ways. In addition to making paper assets more secure, employees with clean desks are more apt to be productive because they can quickly—and safely—access the tools and resources they need to do their jobs.

Common Messy Desk Mistakes

- Leaving computer screens on without password protection
- Leaving documents, mobile phones, USB drives and personal items out in the open
- Neglecting to shred documents before they go into the trash or recycling bin
- Failing to close and lock file cabinets
- Writing usernames and passwords on visible slips of paper or sticky notes
- Displaying calendars for all to see



Email Threats

Social engineering is a non-technical, malicious activity that exploits human interactions to obtain information with the intent to gain access to secure devices and networks. Such attacks are typically carried out when cybercriminals pose as credible, trusted authorities.

An example of social engineering is an email where an employee is asked to contact a tech support hotline and is tricked into giving up credential information.

Phishing Email Compromises

One of the most common forms of social engineering is email phishing—an attempt to acquire sensitive information such as usernames, passwords and credit card data by masquerading as a trustworthy entity. Phishing is a key threat for employees. Such emails often spoof the company CEO, a customer or a business partner and do so in a sophisticated, subtle way.

Common Phishing Techniques

The scope of phishing attacks is constantly expanding, but frequent attackers tend to utilize one of these email tactics:

- Embedding links that redirect users to an unsecured website requesting sensitive information
- Installing Trojans via a malicious attachment
- Spoofing the sender address to appear as a reputable source and requesting sensitive information

How to Block Phishing Attacks

Don't reveal sensitive information

As a general rule, never give out your personal and financial information via email.

Check the security of websites

"http"indicates the site has not applied any security measures while"https" means it has.

Pay attention to website URLs

Look for variations in spellings or a different domain (for example: .com versus .net).

Verify suspicious email requests

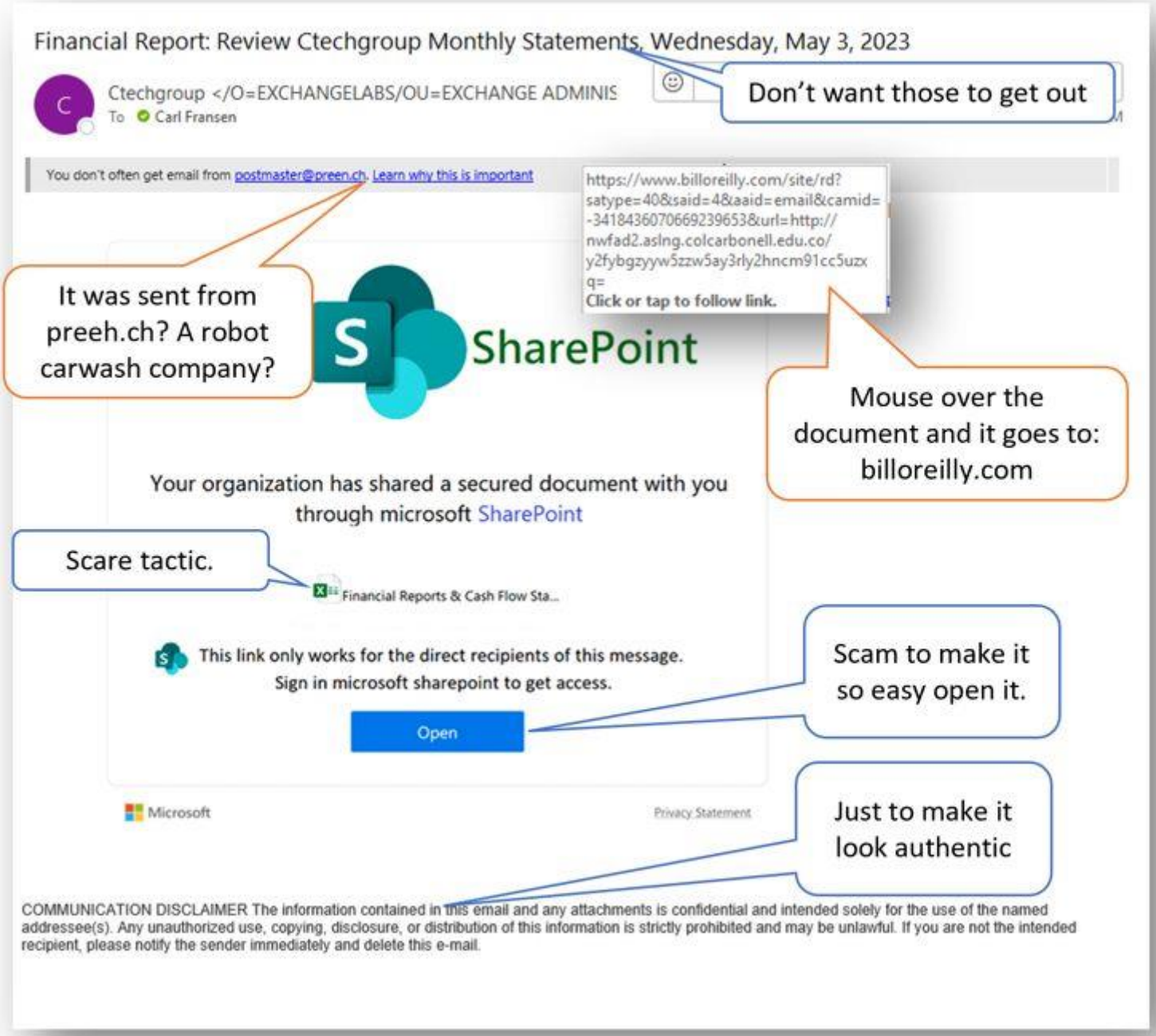
Beware of emails requesting information. Reach out directly to the business through other means.

Keep a clean machine

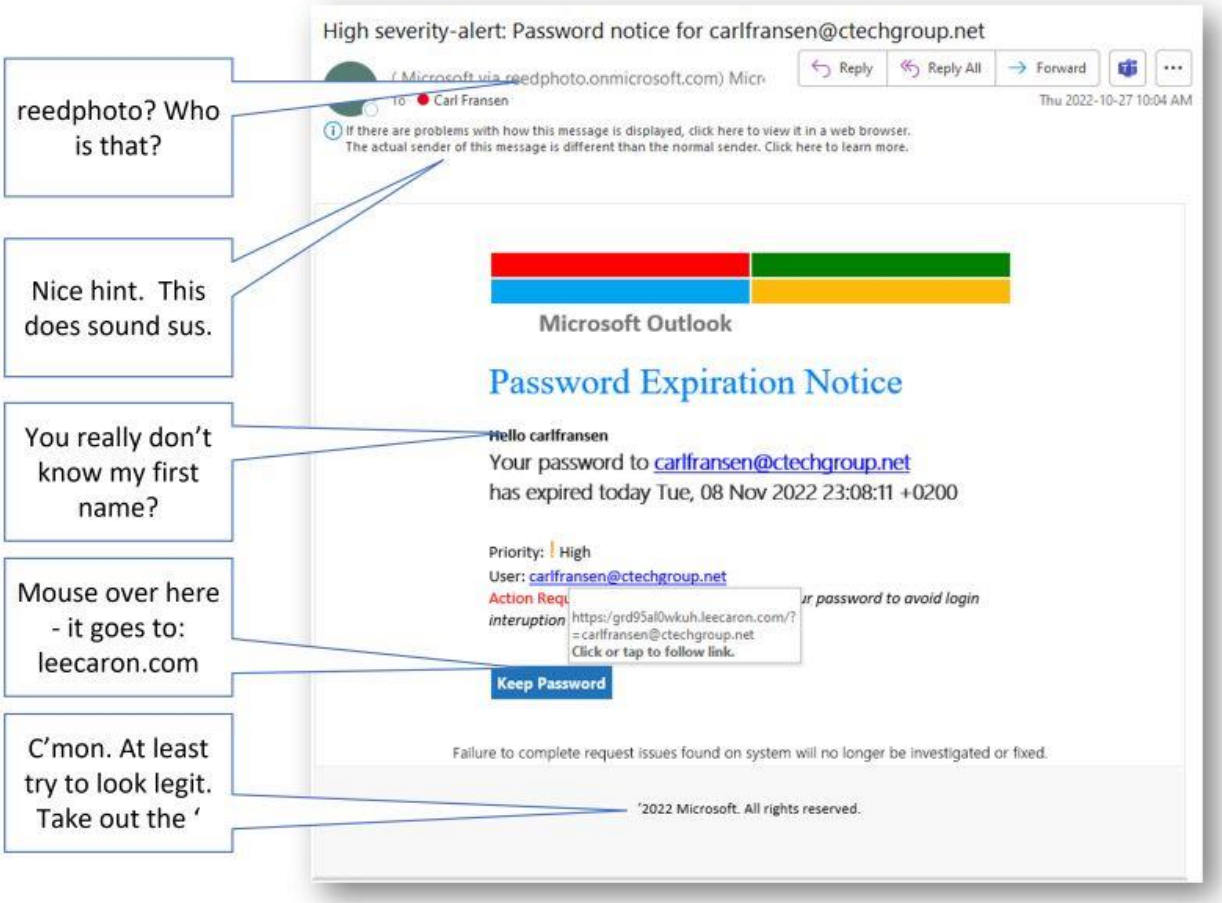
Utilize the latest operating system, software and web browsers, as well as antivirus and malware protection.

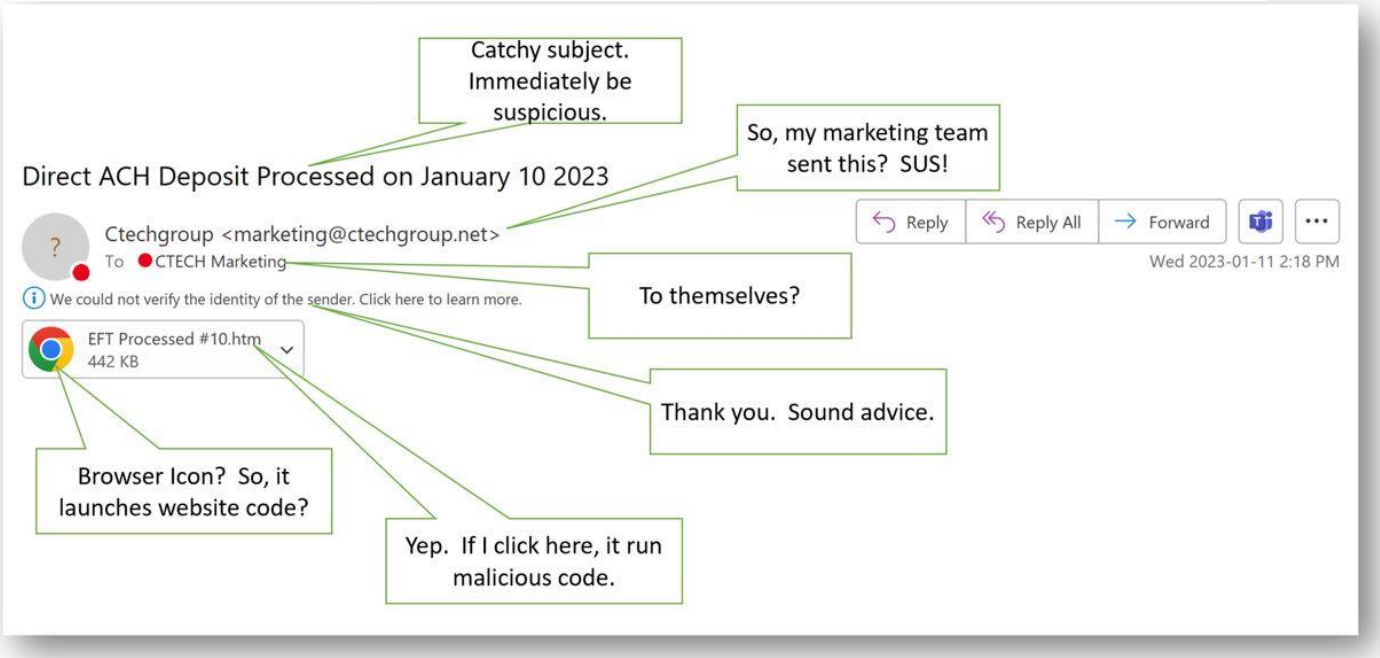
96% According to Verizon's 2021 Data Breach Investigations Report, 96% of cyberattacks arrive by email.

Example


Financial Report: Review Ctechgroup Monthly Statements, Wednesday, May 3, 2023
Ctechgroup </O=EXCHANGELABS/OU=EXCHANGE ADMINIS
To Carl Fransen
Don't want those to get out
You don't often get email from postmaster@preen.ch. Learn why this is important
https://www.billoreilly.com/site/rd?satype=40&said=4&aaid=email&camid=-3418436070669239653&url=http://nwfad2.aslng.colcarbonell.edu.co/y2fybgzyyw5zzw5ay3rly2hncm91cc5uzx
q=
Click or tap to follow link.
It was sent from preeh.ch? A robot carwash company?
SharePoint
Mouse over the document and it goes to: billoreilly.com
Your organization has shared a secured document with you through microsoft SharePoint
Scare tactic.
Financial Reports & Cash Flow Sta...
This link only works for the direct recipients of this message.
Sign in microsoft sharepoint to get access.
Open
Scam to make it so easy open it.
Microsoft
Privacy Statement
Just to make it look authentic
COMMUNICATION DISCLAIMER The information contained in this email and any attachments is confidential and intended solely for the use of the named addressee(s). Any unauthorized use, copying, disclosure, or distribution of this information is strictly prohibited and may be unlawful. If you are not the intended recipient, please notify the sender immediately and delete this e-mail.

Example


reedphoto? Who is that?
Nice hint. This does sound sus.
You really don't know my first name?
Mouse over here - it goes to: leecaron.com
C'mon. At least try to look legit. Take out the '
High severity-alert: Password notice for carlfransen@ctechgroup.net
Reply
Reply All
Forward
Thu 2022-10-27 10:04 AM
To Carl Fransen
If there are problems with how this message is displayed, click here to view it in a web browser.
The actual sender of this message is different than the normal sender. Click here to learn more.
Microsoft Outlook
Password Expiration Notice
Hello carlfransen
Your password to carlfransen@ctechgroup.net
has expired today Tue, 08 Nov 2022 23:08:11 +0200
Priority: High
User: carlfransen@ctechgroup.net
Action Requ
interuption
ur password to avoid login
https://grd95al0wkuh.leecaron.com/?=carlfransen@ctechgroup.net
Click or tap to follow link.
Keep Password
Failure to complete request issues found on system will no longer be investigated or fixed.
'2022 Microsoft. All rights reserved.


Catchy subject. Immediately be suspicious.
So, my marketing team sent this? SUS!
Direct ACH Deposit Processed on January 10 2023
Reply
Reply All
Forward
Ctechgroup <marketing@ctechgroup.net>
To CTECH Marketing
Wed 2023-01-11 2:18 PM
To themselves?
We could not verify the identity of the sender. Click here to learn more.
EFT Processed #10.htm
442 KB
Thank you. Sound advice.
Browser Icon? So, it launches website code?
Yep. If I click here, it run malicious code.

Username & Password Management

Although it should be common sense, employees need to avoid the use of passwords that are easy for hackers to guess. Among the top ten worst passwords, according to www.splashdata.com, are those that use a series of numbers in numerical order, such as "123456." The names of popular sports such as "football" and "baseball" are also on the list, in addition to quirky passwords such as "qwerty" and even the word "password" itself.

Here are 10 of the most popular passwords:

123456	Iloveyou	Zaq12wsxr	sunshine	asdfghjk
password1	1q2w3e4r	qwerty123	letmein	1qaz2wsx

Password length Goal

Number of Characters	Numbers Only	Lowercase Letters	Uppercase Lowercase	Upper, Lower Numbers	Upper, Lower, Numbers, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 sec	2 min	5 min
9	Instantly	3 sec	24 min	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 min	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 sec	2 weeks	332 years	3k years	15k years
14	52 sec	1 year	17k years	202k years	1m years
15	9 min	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

How Attackers Exploit Weak Passwords

While most websites don't store actual username passwords, they do store a password hash for each username. A password hash is a form of encryption, but cybercriminals can sometimes use the password hash to reverse engineer the password. When passwords are weak, it's easier to break the password hash.

Here is a list of common word mutations hackers use to identify passwords if they feel they already have a general idea of what the password might be:

- Capitalizing the first letter of a word
- Inserting a number randomly in the word
- Placing numbers at the beginning and the end of words
- Replacing letters like "o" and "l" with numbers like "0" and "1"
- Punctuating the ends of words, such as adding an exclamation mark "!"
- Duplicating the first letter or all the letters in a word
- Combining two words together
- Adding punctuation or spaces between the words
- Inserting "@" in place of "a"

Tips to Strengthen Password Security

- Change passwords at least every three months for nonadministrative users and every 45-60 days for admin accounts.
- Write a full sentence or phrase as a password: letter1-folder2-accounting3-duck4.
- Avoid generic accounts and shared passwords.
- Conduct periodic audits to identify weak/duplicate passwords and change as necessary.
- Pick challenging passwords that include a combination of letters (upper- and lowercase), numbers and special characters (for example, "$", "%" and "&").
- Avoid personal information such as birth dates, pet names and sports.
- Use passwords or passphrases of 12+ characters.
- Do not write your password out.
- Don't use a browser's auto-fill function for passwords.

Two-factor authentication is now considered minimal level of security. After the end users log in, they receive a text message with a passcode to authenticate their ID. This approach ensures that end users not only know their passwords but also have access to their phone.

Mobile Security

Mobile security is an increasing concern as more and more companies adopt Bring Your Own Device (BYOD) environments, which allow end users to connect to corporate networks through their own (often multiple) devices. Businesses must secure these personal endpoint devices that are not completely under their control, and therefore, pose greater risks.

Mobile Device Security Challenges

- **Lost, misplaced or stolen devices:** Remote wiping is key to protecting sensitive business and personal information.
- **Mobile malware:** Hackers are now turning their attention to mobile devices and text messages. Note: While mobile malware affects Google Androids more than Apple's iOS, a few exploits exist for Apple products as well.
- **Unsecure third-party apps:** If breached, they can serve as a gateway to other apps and ultimately the device's operating system.

Employees who utilize unsecured public Wi-Fi are another area of concern. Hackers in the vicinity of or on the same network can overtake a device and capture sensitive data in transit. The end user can then become the victim of a man-in-the-middle attack, also referred to as hijacking. The hacker leverages the device so that it turns into an invasive device against other unsuspecting end users.

How Employees Can Secure Their Mobile Devices

Set a PIN or passcode

This is the first line of defense. If someone wants to access the device, they first need to break the code. Some device manufacturers also provide the option to automatically wipe the device after a few unsuccessful attempts.

Use remote locate tools

Several software solutions help locate lost or stolen devices through GPS and geofencing capabilities. Apple offers a service like this for mobile devices named"Find My iPhone."For Android users, the Android Device Manager offers a similar service.

Keep devices clean

Today's mobile phones are essentially minicomputers, and they need to be cleaned up from time to time. Utilizing an antivirus and malware scanner is always a good idea.

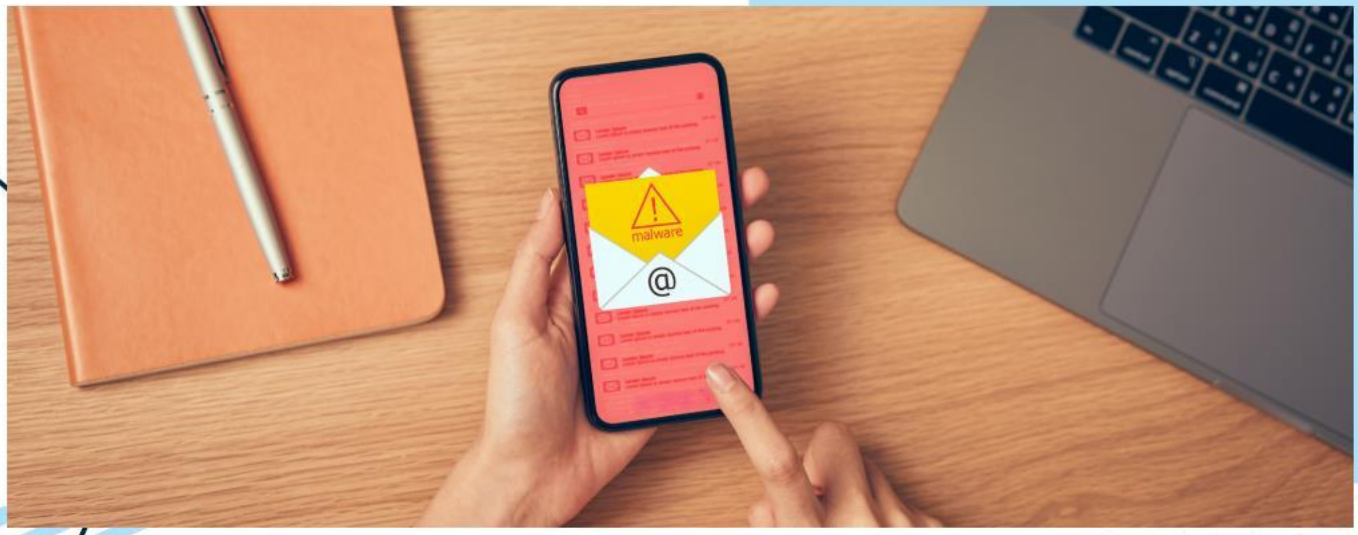
Mobile Device Management (MDM) solutions help businesses and their employees apply these best practices. By deploying an MDM platform, businesses can enforce the use of passcodes, and they can apply geofencing capabilities.

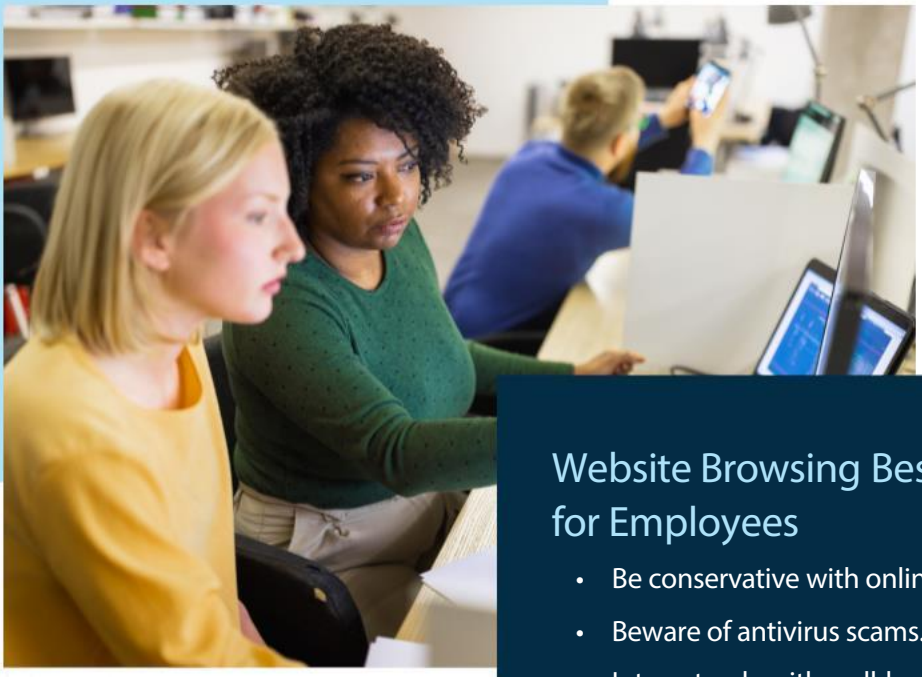
Secure Website Browsing

When end users venture out onto the Internet, it's easy to get tangled up in the vast web of threats. Some threats are readily apparent, but others are well hidden.

Malvertising is a form of malicious code that distributes malware through online advertising. It can be hidden within an ad, embedded on a website page or bundled with software downloads. This type of threat can be displayed on any website, even those considered the most trustworthy.

Another website browsing threat involves social media. According to an article in The Huffington Post, some of the most common Facebook hacks and attacks include click-jacking, phishing schemes, fake pages, rogue applications, and the infamous and persistent Koobface worm. Twitter isn't immune to security issues either. According to CNET News, just 43% of Twitter users could be classified as "true" users. The other 57% fell into a bucket of "questionable"users.





Website Browsing Best Practices for Employees

- Be conservative with online downloads.
- Beware of antivirus scams.
- Interact only with well-known, reputable websites.
- Confirm each site is genuine.
- Determine if the site utilizes SSL (Secure Sockets Layer), a security technology for establishing encrypted links between web servers and browsers.
- Don't click links in emails. Go to sites directly instead.
- Use social media best practices.

!

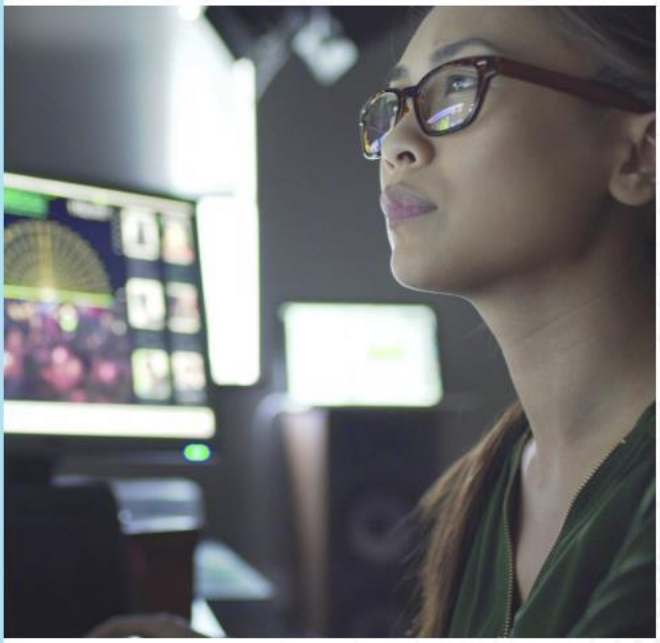
Websites are one of the most common sources of attack. This makes keeping up-to-date browsers paramount for all employees.

The Value of an IT firm to in ensuring Employee Cybersecurity.

They know that having a firewall, password, and antivirus is no longer adequate security. They will use anti-hack artificial intelligence and extend protection to cover not just desktops and servers, but to the cloud services such as Office 365/GSuite, cell phones, and home systems. Also, they provide employee training. As, we have learned, all the tools and solutions in the world can't protect your business from human error.

Here are some of the benefits of working with cybersecurity IT Firm:

- Employ behavioral AI to determine and respond to hack attempts.
- Protect entire threat landscape such as the home and Office 365, Salesforce, Google Suite, etc.
- Protect individual documents as they leave the organization
- Manage a 24/7 Security Operations Center (SOC) to respond to any threats as they happen



Viruses can also do serious harm to information, so consider MSPs who can provide complete endpoint management. Endpoint technology scans downloaded apps and devices for any threats and provides a heads-up if malicious activity is detected.

Education & Technology – a Winning Cybersecurity Combination

Strengthening your business'cybersecurity posture begins with educating your employees. The tips provided within this eBook can go a long way in making sure sensitive information does not fall into the wrong hands. In today's world of advanced hackers, your confidential information is at risk, but a comprehensive cybersecurity defense can stack the odds in your favor.

Let's talk about your needs and how we can help!

CTECH Consulting Group Inc.
Station M Box 231, Calgary, Calgary
T2P 2H6

(403) 457-1478
https://www.ctechgroup.net