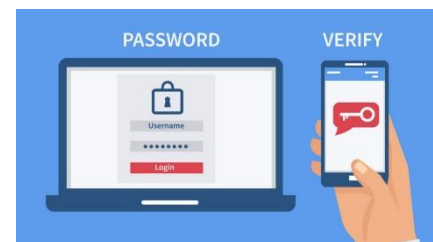




- **Lock** your device with a PIN or password when you leave it.
- Keep your **antivirus and malware program** up to date.
- **Scan** for virus.
- Maintain a **firewall**.
- Avoid **third-party app stores** (be careful what software you download).
- Keep your operating system (**Windows**) and your **software** up-to-date.
- Use **two-factor authentication** for banking (password and pin on mobile phone).
- Back up your data in the **cloud**.
- Don't click on **links** or **attachments** from suspicious emails.
- Learn how to detect **phishing emails**.
- Practice **safe browsing** with https (information exchange is not accessible for third parties)
- Choose a **strong password phrase**.
- Avoid using **public wireless**.
- Keep your **privacy settings** on.
- **Password secure** your private network.
- Make **online purchases** from secure sites
- Be careful what you post.
- Be careful who you **meet online**.
- **Disable bluetooth** when you don't need it.
- Turn **off your computer completely** when you don't need it anymore.

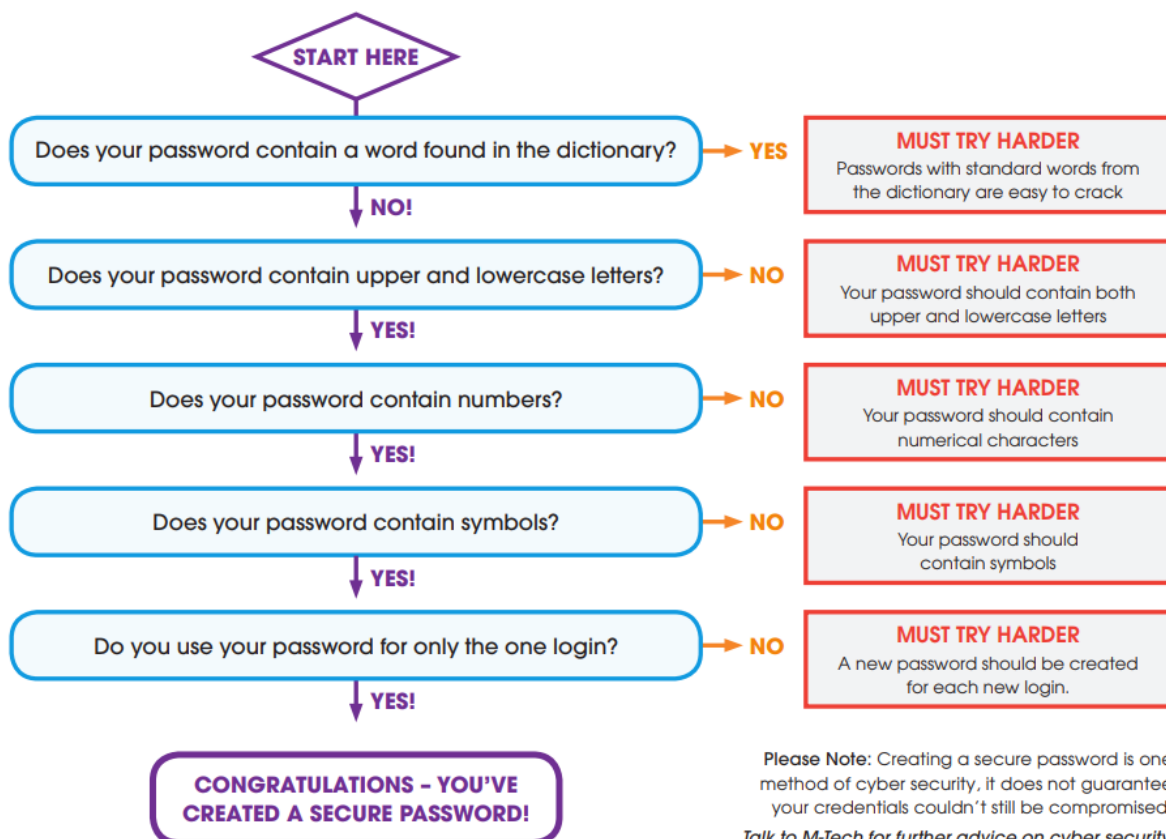


Change your Safe Browsing settings

1. On your computer, open Chrome.
2. At the top right, select More ⋮ > Settings.
3. Click Privacy and security > Security.
4. Select the level of "Safe Browsing" you want to use.

SHOPPING SAFELY ONLINE

- SHOP ON TRUSTED WEBSITES, CHECK THE SELLER
- READ CUSTOMER REVIEWS
- CHECK SHIPPING TERMS AND RETURNS POLICY
- CREATE STRONG PASSWORDS
- AVOID PUBLIC WI-FI, USE A SECURE CONNECTION
- USE ONLY SECURE SITES: LOOK FOR A URL ADDRESS BEGINNING WITH HTTPS INSTEAD OF HTTP
- PROTECT YOUR DEVICES FROM MALWARE
- WATCH OUT FOR SCAMS AND FRAUDS
- CHECK YOUR BANK STATEMENTS REGULARLY
- NEVER USE A DEBIT CARD TO SHOP ONLINE
- BE CAUTIOUS ABOUT HOW MUCH PERSONAL INFORMATION YOU PROVIDE



Detecting a Phishing *Email*

10 Things to Watch

With the uptick in ransomware infections that are often instigated through phishing emails, **it's crucial to take proactive measures to help protect yourself and your organization's security.**

Having a computer that is up to date and patched makes a big difference in reducing an organization's overall risk of infection.

But being vigilant in detecting phishing emails and educating employees in your organization to also be proactive is a critical step in protection.

Here is a quick top ten list for how to spot and handle a phishing email.

1 Don't trust the display name of who the email is from.



Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look at the email address to confirm the true sender.

6 Beware of urgency.

These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a \$1M wire transfer, a Nigerian prince is in trouble, or someone only needs \$100 so they can claim their million-dollar reward).



2 Look but don't click.



Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it—report it.

7 Check the email signature.

Most legitimate senders will include a full signature block at the bottom of their emails.



3 Check for spelling errors.



Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be.

8 Be careful with attachments.

Attackers like to trick you with a really juicy attachment. It might have a really long name. It might be a fake icon of Microsoft Excel that isn't actually the spreadsheet you think it is.



4 Consider the salutation.



Is the address general or vague?
Is the salutation to "valued customer" or "Dear [insert title here]?"

9 Don't believe everything you see.

If something seems slightly out of the norm, it's better to be safe than sorry. If you see something off, then it's best to report it to your security operations center (SOC).



5 Is the email asking for personal information?



Legitimate companies are unlikely to ask for personal information in an email.

10 When in doubt, contact your SOC.

No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than to put the organization at risk.

