Cybersecurity Awareness

THE ANSWER COMPANY

Passwords

- Use strong passwords
- The best passwords contain a mixture of upper-case letters, lower-case letters, special characters and numbers. They should be more than six characters long.
- Change your password regularly
- Password Managers can help you keep track of all of your passwords for you. Use a reputable online program (ie. Lastpass).
- Where possible, use two-factor authentication. This involves an automated email, text message or authenticator application that is sent when a login attempt is made. You receive a code that can be entered on the website/application to complete the login.
- Avoid using work computers for personal use. If you do log in to personal sites, it is best not to have the same password for your personal accounts that you use for work accounts.

WiFi

- Using your home router? **Make sure to reset the default password.**
- Avoid using public networks.

Unsecure sites

- Check the address bar of your browser for **https://** or a padlock icon.
- This means that the site is known to be secure.

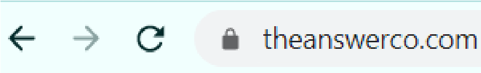
Weak Password

password123

Strong Password

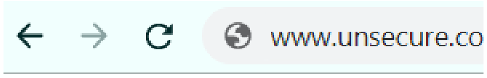
N0t-an-EASYp@ssword

Secure Site



theanswerco.com

Unsecure Site



www.unsecure.co

Mobile devices

The vast majority of us have a cellphone and know that there is a treasure trove of information stored within it about us, our families and friends, our banking, our health and every location we've been to recently. Often, work emails and instant messaging are used on personal devices. This makes them attractive targets for hackers.

- Turn off Bluetooth and WiFi when not using it. Ensure you're connecting to a reputable WiFi network.
- Only download apps available through the Play Store or Apple Store
- Avoid common or standard-issue passwords, like 0000. Most new phones have fingerprint scanners. However, it is advisable to still use a PIN to protect your device.
- Update your phone regularly. New updates usually fix issues with security, so they're crucial!

Shadow IT

You may have had to get up and working from home quickly. There may be areas where security protocols have been bypassed in the name of speediness. For example, you might have used your own cloud storage account to move or store files, or be emailing colleagues from your personal account. This is referred to as "Shadow IT". **Gartner estimates that roughly one-third of all cyberattacks on businesses is due to Shadow IT**. Avoid this as much as possible. Stay out of the shadows.

THE ANSWER COMPANY

Phishing

Phishing is one of the most common methods of hacking. Usually, hackers make themselves appear legitimate in an attempt to trick you. These will often look like they're from services you use, like your bank, or Netflix.

They may also attach files that appear to be legitimate invoices or emails. When clicked, a malicious file is silently downloaded to the computer, giving the hacker access to the whole computer. This means that every device on your network could become infected very quickly.

Before you click any links or attachments in an email, take some time to examine it. Ask yourself, were you expecting this kind of attachment? Is the sender known to you? Does the domain after the @ symbol look correct? For example janedoe@answer.com instead of jabedoe@theanswerco.com. Does anything strike you as odd about the writing? For example: misspelled words or improper grammar.

When in doubt:

- Contact the sender directly by another method (phone, instant messaging, etc.)
- Find the web address or email address from a verified source
- Never open any attachments without verifying them first
- Manually type in the web address of the site instead of clicking on the link
- Verify the email address by hovering over the email address in the "From" section of the email

What to do if you think your computer is infected

The first thing you should is disconnect from the internet. The second thing is to shut down the computer. This is especially important if you have contracted a crypto-virus. These virus cannot run if the computer is off.

→

Next, if you are using a computer owned by your organization, you should reach out to your IT team. Let them know it is urgent.

If there is no in-house IT, now is the time to outsource.

→

Don't log in to any services if you believe your computer is infected.

Ransomware

Ransomware is a virus that infects your computer and allows the hacker full control, meaning you're locked out. Largely, these are downloaded to a machine as a result of clicking on a phishing email. Once the hackers have gotten complete control, they will demand payment in exchange for the return of control. Hackers may threaten to release sensitive data if their demands aren't met. They will often demand the ransom in a cryptocurrency like Bitcoin, which is much harder to trace.

We have even seen cases where ransomware encrypted the data. Once the ransom was paid, a decryption key was provided. However, some of the data was still ruined, and unrecoverable.

While hackers have found many ways to infect computer systems, an enterprise backup program is the first and best way to recover from an attack. But this is not the only way to migitate the damage.

Make sure your antivirus is up-to-date and running – **don't ignore the update alert that's been popping up.**

C-Suite Fraud

Also called business email compromise attacks (BEC), this type of attack is incredibly effective – and there is no virus, no strong-arming at all. All it takes is an email that appears to come from someone in your organization that has some authority. The email will look normal and will ask employees to transfer company funds to a bank account.

Just how effective is it? **In 2019, companies suffered losses estimated at $1.77bn in the US alone (FBI figures).**

The best way to tackle this is directly reaching out to the colleague and confirming that this is a legitimate ask from them. Do this via phone or video call, something that cannot easily be spoofed.

If you need to do it by email, don't reply directly. Start a new email and add the email address from your contacts.