PROTECT YOUR BUSINESS FROM FRAUD AND SCAMS

Malware is intrusive software, often installed without your knowledge or permission, designed to cause damage and disruption to your device or network. It can steal passwords, delete files and is used most often for financial gain.

Examples

A bot

This is a computer that's been infected with malware so it can be controlled remotely by a hacker. Harmful bot activity includes:

- Keylogging, screenshots and webcam access
- Spreading other types of malware
- Sending spam and phishing messages

Adware & Scams

Adware is one of the better-known types of malware. It serves pop-ups and display ads that often have no relevance to you. At best, it's annoying and slows down your machine. At worst, the ads link to sites where malicious downloads await unsuspecting users. Adware can also deliver Spyware and is often easily hacked, making devices that have it installed a soft target for hackers, phishers and scammers.

Phishing & Spam

This is a common method of cyber-attack. Phishing is successful since the emails sent, text messages and web links created look like they're from trusted sources. They're sent by criminals to fraudulently acquire personal and financial information.

Some are highly sophisticated and can fool even your most savvy users. Especially in cases where a known contact's email account has been compromised and it appears, you're getting an instruction from your company, your bank or IT. Others are less sophisticated and simply spam as many emails as they can with a message about 'checking your bank account details'.

Do not click on these links because it will lead you to a site that may look like your account. You will be misled into typing in your username and password – thereby giving them access to your account information.

Ransomware

Denies or restricts access to your own files. Then it demands payment in return for letting you back in. Protect yourself.

- Always keep your Operating System up to date

- Keep your Anti-Virus software up to date
- Back-up your most important files
- Don’t open attachments from unknown sources

Spyware

Secretly records your online activity, harvesting your data and collecting personal information such as usernames, passwords and surfing habits.

Spyware is a common threat, usually distributed as freeware or shareware that has an appealing function on the front end while extracting data in the background. It’s often used to carry out identity theft and credit card fraud.

Once on your computer, spyware relays your data to advertisers or cyber criminals. Some spyware installs additional malware that make changes to your settings.

Trojan Horses

A malicious program that is disguised as a legitimate file. Because it looks trustworthy, users download it. Trojans need a host to work. Harmful activity includes:

- Delete, modify and capture data
- Harvest your device as part of a botnet
- Spy on your device
- Gain access to your network

Viruses

Unlike worms, viruses need an already-infected active operating system or program to work. Viruses are typically attached to an executable file or a word document. An .exe file extension could lead to issues if it’s not from a trusted source. Usually spread via infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated. Once that happens, the virus is able to replicate itself and spread through your systems.

For computer viruses, your contact list is the equivalent of a packed train for the common cold. It hijacks your applications and uses your own apps to sneeze all over everyone… sending out infected files to your colleagues, friends and clients. Because it looks like it’s coming from a trustworthy source (you!), it has a much higher chance of spreading.

Worms

Worms are spread via software vulnerabilities or phishing attacks. It can infect the device or worse, your whole network. Worms can

- Modify and delete files
- Inject malicious software onto devices

- Replicate themselves over and over to deplete system resources
- Steal your data
- Install a convenient backdoor for hackers
- They can infect large numbers of devices fast, consuming bandwidth and overloading your web server as they go.

How you do know if your malware

- A sudden appearance of pop-ups with invasive advertisements. ...
- A puzzling increase in data usage. ...
- Bogus charges on your bill. ...
- Your battery runs down quickly. ...
- Your contacts receive strange emails and texts from your phone. ...
- Your phone is hot. ...
- Apps you didn't download.

How to protect yourself

- Check your social media privacy settings. You can prevent online identity fraud by making sure you have your privacy settings on your social media set appropriately.
- Be wary of unsolicited messages.
- Choose strong and different passwords.
- Be careful when using public Wi-Fi.
- Always do the required updates on your devices
- Install reliable anti-virus software
- If you receive notification that banking details have changed, confirm this telephonically. Call the company on the registered number, not the number which may be given on the same illegitimate e-mail.
- An easy method of verifying an e-mail is to check the domain. If an e-mail comes from example@centrafin.co.za the domain "@centrafin.co.za" indicates that it is legitimate. An e-mail from centrafin@notme.co.za or centrafin@checkagain.com the domain does not belong to Centrafin and could easily be a free site that allows for any e-mail address to be created to deceive clients.
- Be vigilant and look for anomalies - check the email domain, the email address, who is cc'd, email subject, email body, email signature and tone of the email (if it's from a friend but it doesn't seem like their usual e-mail).
- Learn and utilise available IT security tools
- Familiarize yourself with the usual business "day-to-day" e-mails, so that anomalies will be easier to spot.
- If you receive suspicious e-mail purporting to be from Centrafin – report it by forwarding it to Info@Centrafin.co.za

- Shred your personal information

How we are working to protect you

We value our clients and protecting your personal information is very important to us.

- Our information security management is in line with the international standard - ISO27001.
- We have invested substantially in being paperless as far as possible.
- We have secured our networks and website for our protection and yours.
- We encourage engagement with our customers.
- We have implemented systems and procedures to ensure maximum protection of your personal information.
- The right to be forgotten in POPI (Protection of Personal Information) only allows for deletion of personal information that is “inaccurate, irrelevant, excessive, out-of-date, incomplete, misleading or obtained unlawfully.” We regularly scan our databases to ensure that our information is correct.
- We shred all documents after the prescribed period of retention.

To read more about our privacy policy please see the privacy policy on the website.

References

https://comtact.co.uk/blog/what-are-the-different-types-of-malware/
https://www.michalsons.com/