TECH SECURITY HANDBOOK

HOW TO EFFECTIVELY SECURE YOUR NETWORK, DATA, COMPUTERS, AND HOW TO MITIGATE AGAINST CYBER ATTACKS IN 2022

Pctronics

Well today is your lucky day. You are now about to read an ebook containing cutting edge principles in network security ranging from simple to complex. If you follow all of these guidelines, your practices of getting attacked are exponentially less.

Don’t put yourself at risk!

CONTACT US

CLICK HERE TO OPEN A TICKET AND WE WILL GET BACK TO YOU WITHIN 24 HOURS

Secure Your Passwords

It may sound almost too easy but having a ***strong*** password is critical. The stronger the password, the less likely a “brute force” attack can break through.

What is a “Brute Force” attack?

A Brute Force attack is when a program tries to log in with every combination of letters, numbers, and characters until it guesses correctly. This may take the hacking program days, weeks, months, years or even *thousands* years depending on how long and complex your password is.

How to craft the ideal password

While no password is perfect or completely unguessable even by the most unrelenting brute force program, you can help mitigate attacks by having passwords that are:

- 10 characters in length as a MINIMUM
- Using a combination of capital letters and lower case letters
- Use numbers
- Use special characters like . : , / ? # $ &
- DON’T leave your password written on a post-it note around your desk or on your monitor!

It is good practice to change your passwords every 3 to 6 months.

Be Aware of Scam Emails, Pop-ups, or Phone Calls

Hackers have become smart over the years. Remain vigilant of unexpected yet convincingly worded emails or calls that may trick you into clicking links or attachments.

Examples of “shady” messages:

- When the sender’s email address isn’t recognized:

  for instance an email from “Chase Bank” that doesn’t end in @chase.com or that doesn’t have “chase.com” alone somewhere towards the end of the address.

  no-reply@alertsp.chase.com **GOOD**
  info@chasebankalerts118.com **BAD**

- Any phone call or email that you receive that tells you that your network has been hacked and that they can “fix it” if you install some program. Typically this program will allow the hacker to easily remote in to your computer can cause harm.

IF YOU DO NOT RECOGNIZE THE EMAIL, DO NOT OPEN ANY ATTACHMENT!

The moment you open a malicious attachment, it could already be too late.

Other Scams and Phishing Schemes

What is Phishing?

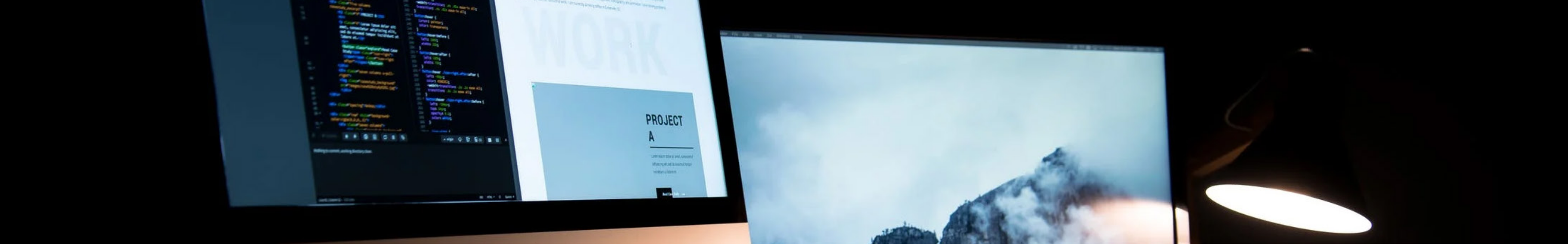
Phishing is the practice of sending emails or directing people to fraudulent pages appearing to be from reputable sources or companies in order to induce individuals to reveal personal information, such as passwords, credit card numbers, and social security numbers!

ALWAYS look at the URL before entering any vital information

Example Scenario:

You may receive a text message or an email claiming that your account has been compromised and that you need to verify your login in order to continue use.

Then you find out that the email you received this notification from has a “shady” URL, like chasebankalerts118.com instead of chase.com and that email has a link that takes you to a login page virtually **IDENTICAL** to the true chase.com login page.



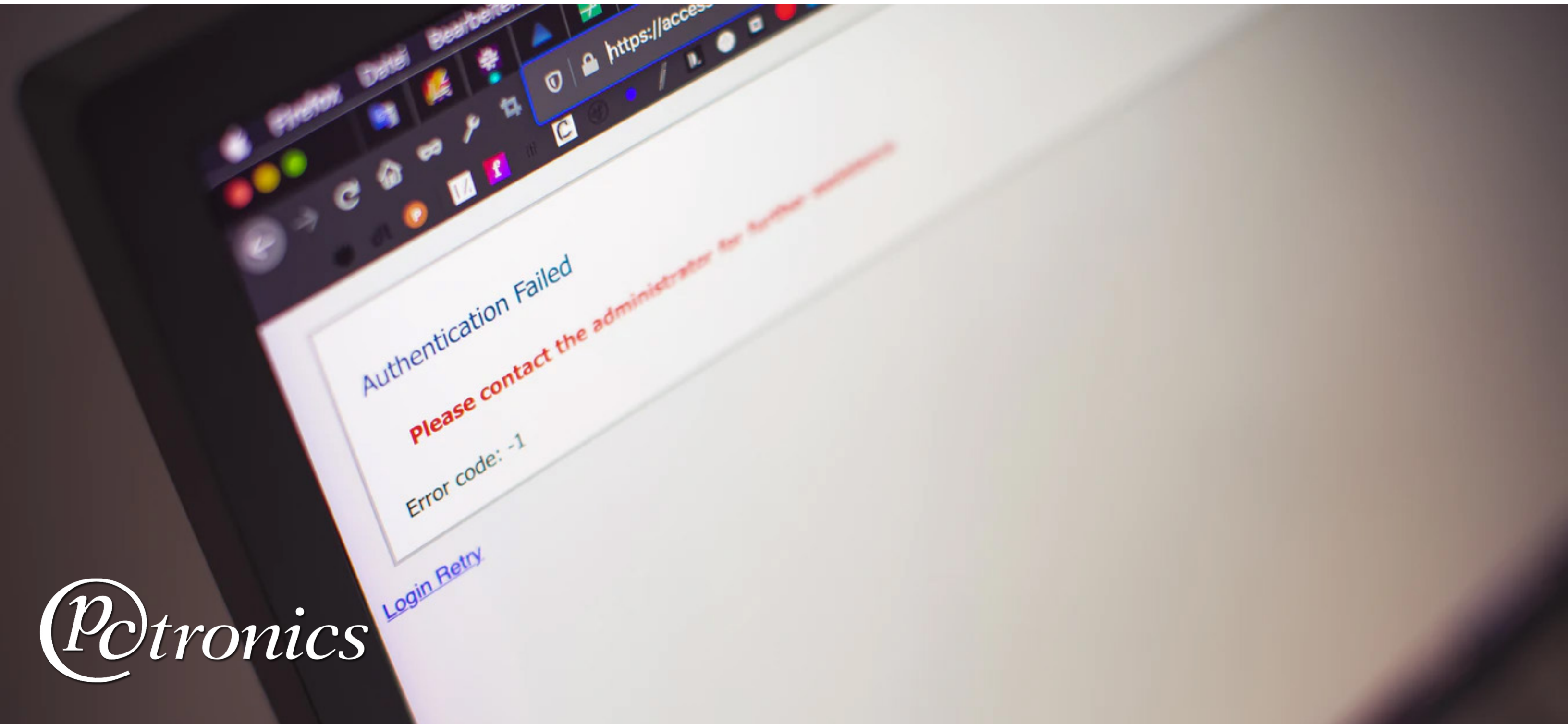
Limit User Permissions

Only request access to resources and shares you actually need to work in

If your data is on a network or in-house server, only allow trusted users to request access to the files, documents, and directories who are directly involved.

DO NOT make anything open to the public that doesn't need to be. **Even one open directory could leave your entire network vulnerable to hackers.**

It is CRUCIAL to have an IT professional assist with these permissions to ensure that it is done correctly.



Authentication Failed

Please contact the administrator for further assistance

Error code: -1

Login Retry

PCtronics

Limit Account Permissions

Don’t accidentally make every user in your company an administrator!

Having full administrative rights on your local PC or network will allow a potential infection to do more damage to systems (unbootable) and data (ransomware attack encrypts data) than if the user account does not have administrative (change system files and settings) rights.

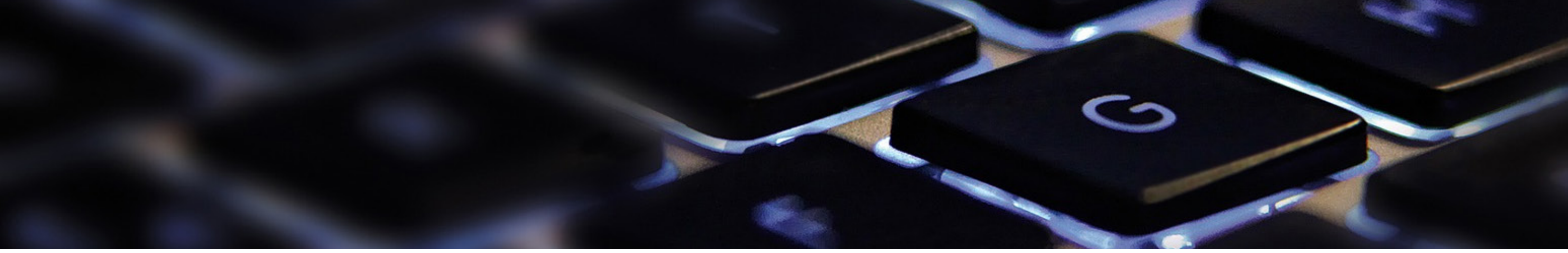
Why this is important...

If one user in your company hasn’t read this ebook and clicks on a malicious link in an email, only that user’s PC would be compromised.

If that user also happens to be an administrator of the entire company network, the hacker now has access to everything.

YOUR ENTIRE NETWORK
WOULD BE COMPROMISED

⚠



Limit Direct Exposure of Systems to the Internet

Remoting into office or work PCs is generally convenient (and often necessary) but it's crucial to add additional protection with 2FA (Two-Factor Authentication)

What is Two-Factor Authentication?

Two-Factor Authentication is a security measure that adds an extra step in order to remote in or log in to a system or an account.

Generally this takes the form of a verification email or text sent to a trusted or secure email.

EXAMPLE: You want to remote in to your work PC from home. When you input your login credentials, you receive an email or text message confirming that there was a login attempt with a link that, when clicked, allows you to finally remote in.

Hackers would not be able to get past this security measure unless they have access to the email or phone to which the 2FA sent the verification.

It is CRUCIAL to have a trained IT professional assist with this set up process to ensure that it is done correctly.

Use a managed or Windows 10 Antivirus software

If you are using Windows 10 Antivirus or Windows Defender:

Make SURE to keep your Windows 10 Antivirus or Windows Defender up to date whenever an update comes out.

If you hare using a professionally managed antivirus program:

- Keep your subscription current. This will allow you to keep your antivirus updated
- Never miss an update
- Always stay informed with the latest information regarding your paid antivirus

Should I get a paid Antivirus or is Windows 10 built-in Antivirus enough?

Windows Defender provides a good basic level of protection but third-party software can have benefits in areas that Windows Defender could lack. Make sure you do your research before committing. We have experience in numerous antivirus software suites and can provide expert advice to guide you.

Just as viruses in real life evolve and build up resistance to medications and treatment, requiring new vaccines and drugs, hackers will evolve their computer viruses as well. **ALWAYS KEEP YOUR ANTIVIRUS UP TO DATE.**

Keep all computers current with latest updates

Microsoft regularly releases cumulative updates around the 10th of every month. System/server restarts might be required.

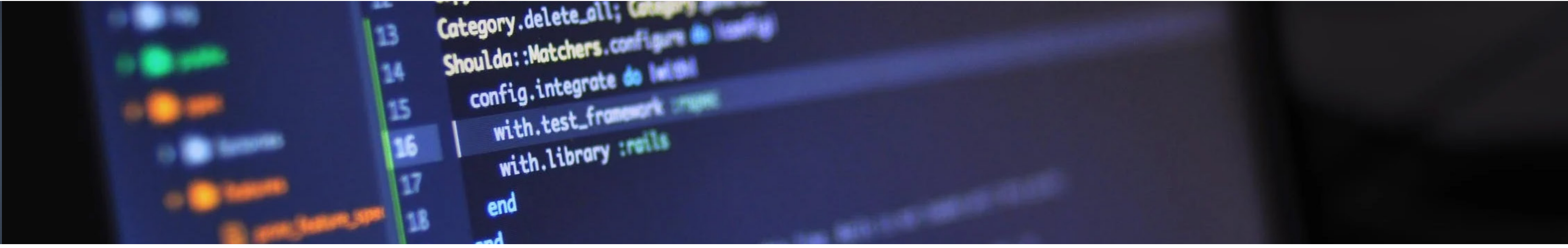
Just as antivirus programs must be updated, there are also mechanisms within the Windows 10 framework that require updating frequently.

If you do not keep your PCs updated, your computers (and network) could be vulnerable to **attacks that won’t even be detected through antiviruses.**

But don’t the Windows 10 updates happen by themselves?

Yes and no. Sometimes you’ll get lucky and your system is set up to have all of the right updates to occur automatically. Other times, some updates - even critical updates - will need to be done manually ***and these are the ones that generally go unnoticed.***

Furthermore, sometimes Microsoft likes to add in unneccesary programs along with their updates. They’re not malicious, just often annoying (X-Box, 3D Viewer, random Music Players etc.). These can be avoided by doing updates manually.



```
Category.delete_all;
Shoulda::Matchers.configure do |config|
  config.integrate do |with|
    with.test_framework :rspec
    with.library :rails
  end
```

Do not download and install unknown or unsolicited programs/apps

IMPORTANT IF YOU ARE A SYSTEM ADMINISTRATOR

If your PC has limited permissions (and is unable to download or install without the go ahead from a system administrator) this will not be a significant issue.

However, if your PC is the system administrator, DO NOT download anything you do not recognize. DO NOT install any program you do not recognize, and DO NOT click on anything you do not recognize.

It does not matter how blatantly obvious or how hidden a piece of malicious software is, the second you allow the program to install...

IT MAY BE ALREADY TOO LATE

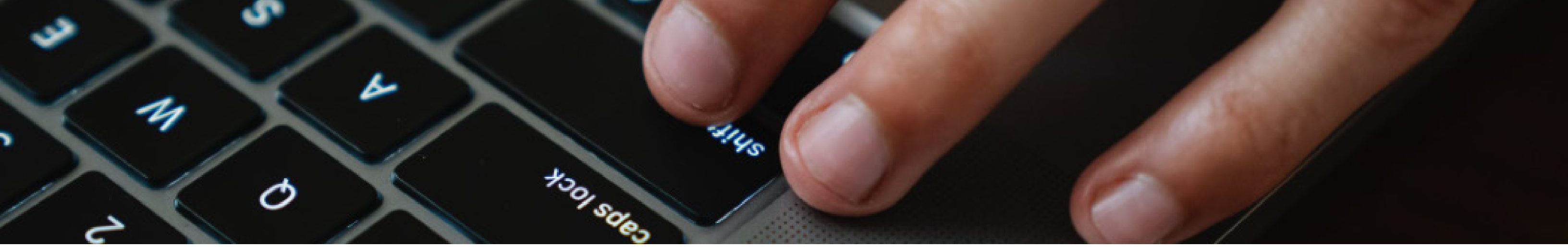
Keep Your Data Backed Up

Most user data should reside on servers, as it is common practice to have redirected ***user profile*** folders in place such as desktop, documents, and photos, to server shares.

Check backup logs and swap backup drives daily. If a server gets infected and needs to be restored, you will lose only one day's worth of work/data if the drives are swapped daily.

Configure laptops with Microsoft OneDrive to auto-backup desktop, documents, and pictures to cloud.

It is CRUCIAL to have a trained IT professional assist with this set up process to ensure that it is carried out correctly.



Shut Down, Log Off, or Lock Your Systems Regularly

You can easily prevent unauthorized access to your PC or Mac before leaving the systems unattended.

How to quickly lock your system

Lock your PC with (Win + L) or Macs with (Apple logo – Lock Screen). In both cases, Windows and Apple offer automatic locking features (Windows Dynamic Lock, Apple Screen Saver/Hot Corner).

Why this is important...

This prevents hackers from remoting in to a user's computer unless they know the user's login password already. **Most hacking attempts are only possible when a system is on and accessible.** Turning it off when you're not using it or logging out is a good line of defense against malicious attacks.

Data Security and Tips

Here in the digital age, hackers aren't going away. In fact, they are only becoming more prominent, smart, and creative in their ways of getting in to your systems.

We at PCtronics can assist you with any questions you may have in securing your networks and computers, and we can provide security audits of your networks and computers as well as develop recommendations.

If you have any questions or concerns regarding your PCs or network security, please give us a call at (949) 407-7570 or email us at helpdesk@pctronics.us.

CONTACT US

CLICK HERE TO OPEN A TICKET AND WE WILL GET BACK TO YOU WITHIN 24 HOURS