En bild som visar inomhus, bärbar dator, dator, sitter

Automatiskt genererad beskrivning



Basic Cybersecurity

October 2020

During ESCM, **European Cybersecurity Month**, SRS has published practical advice and tips to raise cybersecurity awareness. Our cybersecurity tips have focused on actions that can be done within the areas people, processes, and technology. Below you will find our tips summarised under

* Passwords
* Connected devices
* Apps, programs, and other services

Passwords

Your password is a virtual key that prevents unauthorised access to your accounts and should be treated as a valuable document.

Create secure passwords. The 15 billion most common passwords are leaked and for sale cheaply online. If you use any of these passwords, it will severely weaken the security of your accounts. To avoid this, always create unique and separate passwords for each system and website. See the paragraph below.

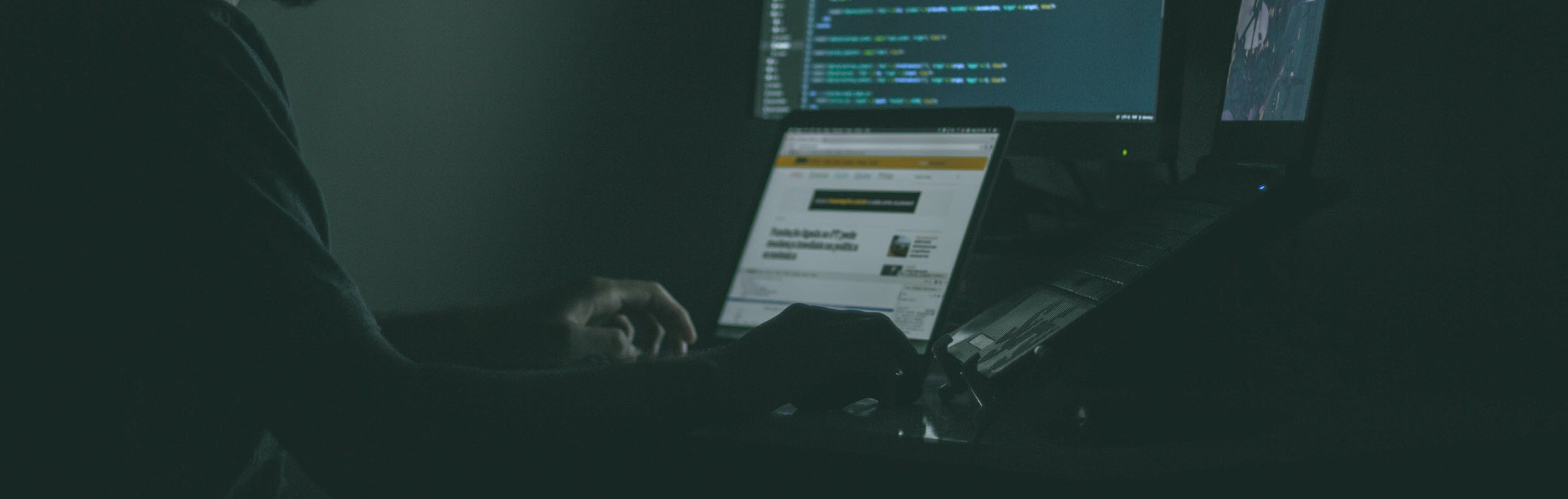
Use a password manager. SRS recommends for example F-Secure Key for generating strong and unique passwords of at least 15 characters. A better gaming computer can make up to 40 billion attempts per second on a password. A password of 9 characters takes about six months to crack, while seven characters only take 28 minutes. If your password is on a list or in a leak, it will only take 0.1 seconds for the password to be cracked; Length and non-predictability of the password matter.

As an organisation:

* Ensure a regulatory framework for which password can and should be set

Regularly test that the passwords within your organisation fulfil set requirements

Enable multi-factor authentication for all online services. Today, the simplest way to make phishing-fraud more difficult is by using two-factor authentication or multi-factor authentication (MFA). To put it briefly, you can increase security by using two different verification steps. Our recommendation is to use an app and not SMS since SMS easily can be hacked and redirected to another SIM card.



Connected devices

The following shall be observed when using connecting devices such as computers, telephones, wireless devices, watches, etc.

Ensure offline backups. Ransomware is malware that encrypts files and requires money in exchange for their recovery. Your backups need to be offline because ransomware viruses do not stop at taking your local files but find their way around the network and encrypt everything they get access to , i.e., the entire IT infrastructure, including the backups that are internally available on your system. SRS recommends making regular backups to external encrypted offline hard drives.

As an organisation:

* Set a regulatory framework for how and with what frequency backups should be done and test to restore from the backups to ensure that it is feasible

Do not connect devices to your network without approval. If a device (keyboard, coffee machine, server, etc.) is connected to the network without fulfilling internal security requirements there is a risk that the device becomes an open door into the system. Once plugged into a strategic location, the entire network risks being tapped.. Be vigilant and question unexpected widgets in conference rooms and office environments.

As an organisation:

* Implement authentication on MAC addresses to prevent unauthorised access
* Continuously monitor networks for unknown devices
* Implement a process for how devices are controlled and allowed

Only connect to wireless networks you trust or use a VPN. VPN helps protect your online privacy by encrypting your traffic. Hackers use internet connection or WIFI networks as a door to access your computer. If you connect to a WIFI network in a café or airport, an attacker can easily see the addresses of the web pages you visit and data from your phone applications. Using a secure VPN makes your traffic encrypted and attackers will no longer access your files. SRS recommends choosing pay VPN services from a provider and a country that you trust. VPN providers can see parts of your unencrypted traffic and free VPN services are likely to sell your data as part of their business model. .

As an organisation:

* Provide your employees with a VPN solution on your work phones

Never plug an external device from someone you don't trust into your computer. Malicious USB sticks are an effective way for attackers to get into a computer and quickly infect it with viruses. In worst case, USB devices can physically destroy a computer by charging the capacitor, which then gives the computer a powerful energy surgedestroying it. Be careful when someone asks for help printing documents from a USB or charging their phone on your computer.

As an organisation:

* Inform your employees about the dangers of external devices so that everyone is aware and careful

Impede tapping by being vigilant and using strong password. Tapping can be done many ways, either through physical presence or through technical solutions. Cameras and microphones can be made extremely small and easily built into cords and devices camouflaged into standard IT-equipment. Vulnerable networks with weak passwords are often taken advantage of to get the information out. This is an easy set-up fort intruder as they can utilise existing infrastructure for transferring data out onto the Internet.

As an organisation:

* Regularly screen conference rooms for cables and devices that should not be there

Turn off (not just disable) location services, WIFI, and Bluetooth when not in use. It is not uncommon for apps and applications to repeatedly ask for access to your location, photos, etc. It is often enough that you click "yes" and then it's on forever, even when you do not want to. When you launch new versions, there may be features that automatically turn on things you do not want. SRS recommends that everything is turned off and that you turn ton things case by case when needed.

Distinguish between professional life and private life. Separate your personal and professional devised as well as entities with protection-worthy information. Do not install apps for private use on your business's equipment or reuse digital assets from your company such as email addresses and passwords..

As an organisation:

* Design policies and guiding principles and train your employees to ensure a self-sustaining security culture



Apps, programs, and other services

The following should be observed when using apps, programs, and other services.

Do not be logged on as an administrator. By not being logged on as an administrator, you reduce technical vulnerabilities by 80-95%. An account with administrator rights has access to the entire computer's vital operating systems and files, and has permission to make changes and access the whole computer system. SRS recommends having a separate account for admin and only use it when necessary.

As an organisation:

* Set-up separate accounts and devices for administration of systems and user rights
* Regularly conduct threat and risk assessments, including assessment of key values

Turn off all macros. Macros are used to automate various functions to facilitate for users to perform specific tasks or view different content. In short, a macro is a series of commands that are recorded so to be played back at a later time. An attacker can write a macro that can do the same things as malware, e.g. stealing data, encrypting files, sending emails to all your contacts, set-off just by you opening a document in Word, Excel, or Powerpoint. Therefore, turn off all macros and only allow macros in documents that are on trusted network locations.

As an organisation:

* Do not allow users to enable macros themselves

Do not wait with making updates. On average, it takes just over a month from an update being released to the start of cyberattacks, whereof 25% occur already within the first week. Therefore, update your systems as soon as possible, preferably within 48 hours.

As an organisation:

* List key assets to determine which are the most critical
* Monitor the systems you use for acute vulnerabilities/updates

The firewall should be turned on, even for outgoing traffic. A firewall is a security tool that filters incoming and outgoing traffic from your device and the Internet. It also prevents information leaks during internal erroneous configurations and hinders malware from being installed and spread. Many understand the importance of having a firewall that protects against incoming traffic but miss to block outbound traffic services.

As an organisation:

* Turn off inbound and outbound traffic for the protocols below and only allow traffic from trusted networks
  + SMB and TFTP /FTP
  + MS RPC and SNMP
  + SMTP and IRC
  + DNS and ICMP
* Configure your firewall to alert if any internal device tries to use TFTP or IRC as this may indicate malware on the network

Do not write anything in an email that you would not write on a postcard. When an email message travels over the Internet, it can be read along the way, just like a postcard. Between the sender and recipient, there are several mail servers and proxies that the message moves between, and once at the destination server, a possible stealth reader can be the email administrator. Use encrypted communication channels for exchanging sensitive information or encrypt the documents containing important information before sending it. Use email encryption such as SMIME or PGP.

Review the cloud services you use. Today, many switch to cloud services but miss both setting security requirements on the provider and doing a proper risk analysis to ensure appropriate security measures. SRS recommends reviewing who the supplier and its owner are; what laws and regulations apply to them? How is their business model? If the service is for free or very cheap, there is a risk that "you are the product". Further you should also assess the supplier's definition of security ; what standards are they working by? What certifications and vetting have they undergone?

As an organisation review:

* Context: What laws and regulations apply to you? What risk appetite does your organisation have?
* Key assets: What information do you want to protect (personnel, reputation, availability, etc.)?
* Threat actors: Whom do you want to protect yourself from, and what are their capabilities?

Protect your files by encrypting them. Encryption is an effective way to protect digital information, either locally on your computer, on your provider's device or in motion. Information in motion means data during transport, movement across a network from one device to another, such as email, chat, or web surfing. When protecting data, it is essential to consider both conditions. For example, an email server or spam filter administrator could normally access and read emails as encryption only occurs between email servers and between the server and your device. SRS recommends encrypting hard drives and USB sticks as well as using encrypted communication channels. Password protect sensitive documents sent across channels that do not have end-to-end encryption (E2EE).

Be careful regarding agreements that you accept. Many apps are both appealing and fun, but unfortunately, these can contain very questionable user agreements that most of us just click past by pressing "Approve". The agreements can include what data that will be collected, what the supplier will have access to, and who will receive the information. In many cases, the agreements change over time. Read the agreement or cosunlt with someone knowledgeable in the field of information security. Expect that passwords and information processed by the app/service will be available to many more than you imagined.

Do not base security on personal data. Especially in Sweden but also in other countries it is easy to get hold of a wide range of private data. . Basing security back-up on questions such as "What is your mother's birth name?" makes it easy for criminal actors to find the answer. One reason for this is that we share a lot of information about ourselves online and on social media. With today's high-resolution cameras, it is especially important to think about what you publish online. It is possible to copy fingerprints and deceive some face recognition from these images. SRS recommends controlling and limiting what, when, and to whom you post and display things.

Be aware of who is trying to reach out to you over SMS, phone, and email. A simple oral answer like "Yes" could lead to someone else buying themselves a car with your money through your consent. Phishing, smishing, vishing, whaling are all part of the concept of "social engineering", which involves athreat actor trying to lure out sensitive information from their victim or get them to click on a link that, in turn, can lead to a device being taken over. These methods are now much more polished than just a few years ago.

As an organisation:

* Maintain continuous safety tests and training for your employees

Educate each other, 80% of all cyberattacks start with an e-mail. Ransomware and crypto viruses are malicious software whose purpose is to blackmail by preventing users from accessing their systems or personal files. To regain access, payment is required. Cybercriminals are almost always just looking for money, and by blocking your information and services or threatening to leak it, they have a direct source of income - you. . SRS recommends disabling macron and only using newer version of the office programs.

Configure SPF to prevent counterfeit domain names. There are free mail servers to run on your computer, where you can specify who the sender should be. Everyone can send emails and declare themselves to @whitehouse.gov. To ensure the sender is correct, the recipient must set up a controls that checsk which servers and computers that are allowed to send you emails. This is called the Sender Policy Framework (SPF) and is a method to prevent email from being sent with forged domain names in sender addresses. Also note that Outlook rarely writes the address within the organisation but only displays names and that mobiles only show display names for all senders, but by replying or clicking the name, you will see the full address.

Do you have questions about your cybersecurity?

Contact us on cybersecurity@srsgroup.se and we will point you in the right direction!