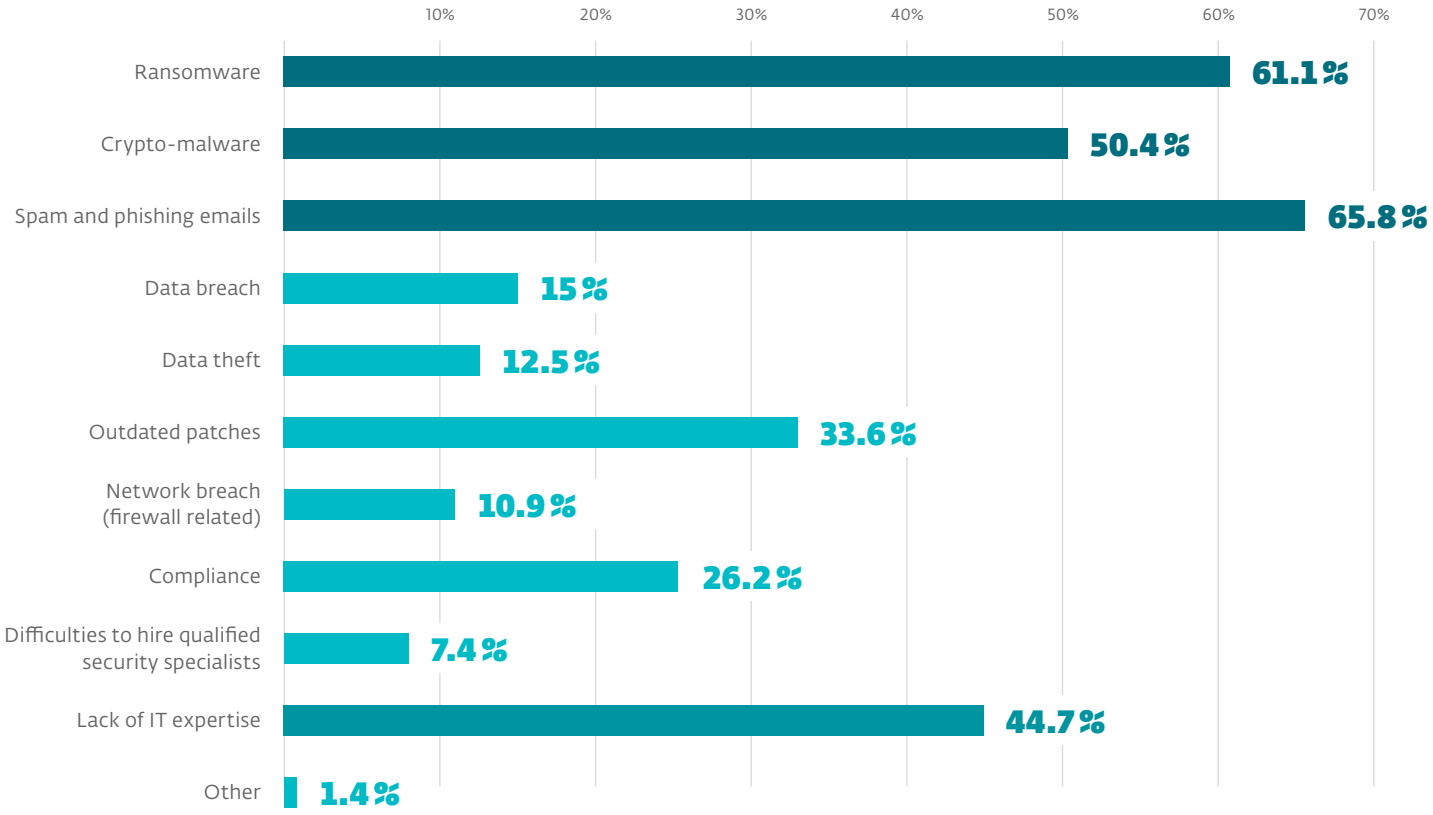
ESET MSP PROGRAM

TOP SECURITY CHALLENGES FOR SMBs

1. RANSOMWARE
2. SOCIAL ENGINEERING
3. ILLICIT CRYPTOMINING
4. PASSWORD SECURITY

Addressing the top SMB security challenges identified by MSPs

We asked our MSP partners about the main challenges they encounter when protecting their customers. Almost 500 MSPS responded, telling us that **ransomware, crypto-malware** and **social engineering attacks**, via spam and phishing emails, are major concerns, as is a **lack of IT expertise**. So we're offering you this useful advice on how you can address these issues.



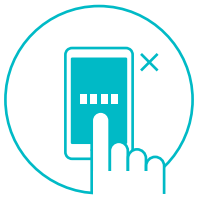
Source: ESET poll of 488 MSP partners in 14 countries during July 2019, via an online questionnaire.

1 Ransomware
How does it work?

There are multiple techniques used by ransomware cybercriminals including:

Screen locker ransomware

blocks access to a device screen, other than to see the malware user interface.



PIN locker ransomware

changes the device's PIN code, rendering its content and functionality inaccessible.

Disk coding ransomware

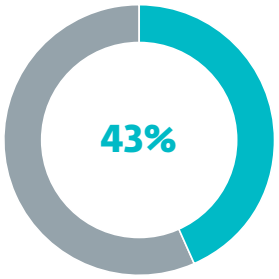
encrypts the MBR (Master Boot Record) and/or critical file system structures, and thus prevents the user from accessing the operating system.

Crypto-ransomware

encrypts user files stored on disk

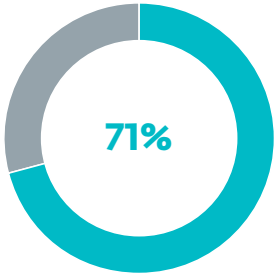
Why should SMBs care?

Small and medium-sized businesses are now increasingly attractive targets for cybercriminals. They are more valuable targets for cybercriminals than consumers, and more vulnerable than large enterprises.



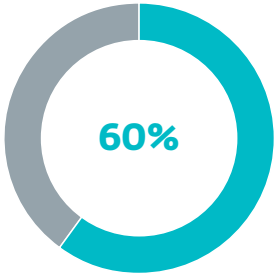
43% of victims in data breaches are SMBs.

Source: Verizon 2019 Data Breach Investigations report (DBIR)



71% of breaches are financially motivated

Source: Verizon 2019 Data Breach Investigations report (DBIR)



60% of victims paid the ransom demanded.

Source: Ponemon 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB) survey

MSPs report the **average ransom demanded from SMBs is ~$4,300** while the average cost of downtime related to a ransomware attack is ~$46,800.

Source: Datto 2018 State of the Channel Ransomware Report

DON'T PAY!

There is absolutely no guarantee that cybercriminals will deliver on their side of the bargain (sometimes they are unable to do so, either intentionally or as a result of incompetent coding). ESET **recommends not paying** the sum demanded — at least not before contacting your security provider's technical support to see what possibilities exist for decryption.

How to keep your systems protected

Basic recommendations

There are a few things that you can do to keep ransomware from wrecking your day. Let's start with what can be done in advance to help prevent malware from getting onto your system in the first place, and to minimize damage if it does happen.

1. **Backup data** on a regular basis and keep at least one full backup of the most valuable data off-line
2. Keep all software and apps – including operating systems – **patched and updated**
3. **Use a reliable, multilayered security** solution and make sure it is patched and up-to-date

Additional protective measures

- **Reduce the attack surface** by disabling or uninstalling any unnecessary services and software
- **Scan networks** for risky accounts using weak passwords and ensure they are improved
- **Limit or ban use of Remote Desktop Protocol (RDP)** from outside of the network, or enable Network Level Authentication
- **Use a Virtual Private Network (VPN)** for remote access
- **Review firewall settings** and close any non-essential ports that could lead to an infection
- **Review rules and policies for traffic** between internal company systems and outside network(s)
- **Password-protect the configurations** of security solutions
- **Segment the company LAN into subnets and connect them to firewalls** to limit lateral movement
- **Protect backups** with multi-factor authentication (MFA)
- **Regularly train employees** to recognize cyberthreats and avoid social engineering attacks
- **Limit shared file and folder access** only to those who need it
- **Enable detection of potentially unsafe/unwanted applications (PUSA/PUA)** in order to block tools that can be misused by attackers to disable the security solution

2 Social engineering
Defining the problem

Social engineering is a category of non-technical attack techniques used by cybercriminals to manipulate users into breaking security or other business process protocols, performing harmful actions or giving up sensitive information.

- **Social engineering techniques typically don't require much technical skill** on the part of the attacker, which allows all types of cybercriminals, from small-time thieves to advanced hackers, to try their hand.
- The damage is real and extensive, which is well-illustrated by the FBI's Internet Crime Complaint Center (IC3) annual report which estimates that in 2018 alone, US companies **lost more than $2.7 billion to cyberattacks**. $1.2 billion of that was attributed to business email compromise (BEC)/email account compromise (EAC), where scammers took control of the legitimate email accounts of senior staff and misused them to order/conduct unauthorized transfers of funds.
- Even some of the most sophisticated cyberattacks in history, such as Black Energy, GreyEnergy or Industroyer, utilized phishing and other forms of social engineering as their initial compromise vectors, **demonstrating the effectiveness of these techniques** and their popularity among cybercriminals.

100% increase in global losses from targeted BEC/EAC scams between May 2018 and July 2019

Source: FBI Public Service Announcement, September 10, 2019. https://www.ic3.gov/media/2019/190910.aspx#fn1

How cybercriminals try to trick us

There are many techniques that fall under the umbrella term of social engineering in cybersecurity. These are the most frequent:

Spam
is any form of unsolicited communication sent in bulk. Most often spam is a commercial email sent to as many users as possible, but can also be delivered via instant messages, SMS and social media. Spam is not social engineering per se, but some of its campaigns utilize social engineering techniques such as phishing, spearphishing, vishing, SMS phishing or spreading malicious attachments or links.

Impersonation
by cybercriminals sees them act in the name of a trusted person in order to deceive victims into taking actions that harm them or their organizations. A typical example is an attacker who impersonates a company's CEO requesting and approving fraudulent transactions.

Phishing
is a form of cyberattack in which the criminal impersonates a trustworthy entity to request sensitive information from the victim, normally by email. Vector-specific subtypes include **vishing** (**v**oice ph**ishing**), which employs fraudulent phone calls, and **smishing** (**SM**S ph**ishing**), which uses SMS text messages containing malicious links or contents. These types of fraud usually try to create a sense of urgency, or employ scare tactics to coerce the victim into complying with the attacker's requests. Phishing campaigns can target large numbers of anonymous users, or a specific victim or small group of associated victims.

Spearphishing
is a targeted form of phishing in which the attacker sends highly-customized messages to a limited group of people, or even just an individual, with the aim of harvesting their data or manipulating them to perform harmful actions.

Technical Support Scams
are usually bogus phone calls or web ads in which attackers offer the victim unsolicited technical support services. In reality, cyber-criminals try to make money by selling fake services and removing non-existent problems.

Scareware
is software that utilizes various anxiety-inducing techniques to manipulate victims into installing further malicious code on their devices, often while extracting payment for non-functional or outright malicious software. A typical example is a fake antivirus product designed to trick users into thinking their devices have been compromised and that they need to pay for the full version that includes cleaning functionality (this can in turn provide a vector for further infection).

How to recognize a social engineering attack

Sense of urgency

The criminals behind social engineering campaigns often try to scare victims into action by using anxiety-inducing phrases such as “send us your details right away, or your parcel will be discarded” or “if you do not update your profile now, we will close your account”. Banks, parcel companies, public institutions and even internal departments usually communicate in a neutral and factual way. Therefore, if the message is trying to push the recipient to act quickly, it is probably malicious and potentially a dangerous scam.

Poor language skills

Typically, attackers don’t pay too much attention to detail, sending messages full of typos, missing words and poor grammar. Another linguistic element that can signal an attempted attack is generic greetings and formulations. So if an email starts “Dear recipient” or “Dear user”, be wary.

Strange sender address

Most spammers don’t take the time to spoof the sender’s name or domain in order to make these look trustworthy. So if an email comes from an address that is a mix of random numbers and characters or is unknown to the recipient, it should go directly into the spam folder and be reported to the IT department.

Requests for sensitive information

Institutions and even other departments in your own company will not normally request sensitive information via email or phone — unless the contact was initiated by the employee.

If something sounds too good to be true, it probably is

This is as true for unsolicited giveaways on social media as it is for that “excellent yet time-limited business opportunity” that just landed in your inbox.

How can your company protect itself from attacks?

There are several things that you and your MSP can do to help protect you from social engineering:

- **Regular cybersecurity training for ALL employees**, including top management and IT personnel. Remember that such training should show or simulate real-life scenarios. Learning points must be actionable and, most of all, actively tested outside the training room: social engineering techniques rely on the low cybersecurity awareness of their targets.

- **Scan for weak passwords** that could potentially become an open door in your organization's network for attackers. Additionally, protect passwords with another layer of security by implementing multi-factor authentication.

- **Implement technical solutions to tackle scam communications** so that spam and phishing messages are detected, quarantined, neutralized and deleted. Security solutions, including many that ESET provides, have some or all of these capabilities.

- **Create understandable security policies** that employees can use and that help them to identify what steps they need to take when they encounter social engineering.

- **Use a security solution and administrative tools,** such as ESET Security Management Center, to protect your organization's endpoints and networks by giving administrators full visibility and the ability to detect and mitigate potential threats in the network.

3 Illicit cryptomining
A hidden threat

An illicit cryptominer is potentially unwanted or malicious code designed to hijack the idle processing power of a targeted device and misuse it to mine cryptocurrency. The mining activity is usually hidden or runs in the background.

There are two main types of illicit cryptominers:

Binary-based cryptominers
are malicious applications downloaded and installed onto the targeted device with the goal of mining cryptocurrency. ESET security solutions categorize most of these applications as Trojans.

Browser-based cryptominers
use malicious JavaScript embedded into a web page or some of its parts/objects in order to mine cryptocurrency via the browsers of the site's visitors. This method is dubbed **cryptojacking** and has become increasingly popular with cyber-criminals since mid-2017. ESET detects the majority of cryptojacking scripts as potentially unwanted applications (PUAs).

Did you know?

Most illicit cryptominers attempt to mine Monero or Ethereum as they offer several benefits over the better-known Bitcoin: they have a higher level of transaction anonymity and, most importantly, can be mined with regular CPUs and GPUs instead of expensive, specialized hardware.

The harm that cryptomining can cause

Due to their higher performance, business-grade hardware and networks are more valuable targets than consumer devices, promising attackers higher earnings within a shorter timeframe.

Despite illicit cryptomining appearing to pose a less severe threat than more invasive attacks, organizations should not underestimate the risk it represents. Mining usually hijacks a large portion of hardware processing power.

This results in:

1. **reduced performance**
2. **lower productivity**
3. **damage to targeted devices** as the power-hungry mining process places additional stress on hardware components, shortening their lifespan.
4. **Cryptominers expose vulnerabilities in an organization's cybersecurity posture** that can lead to severe future compromises and disruptions.

50% of MSPs identify crypto-malware as one of the biggest security challenges they encounter via their customers.

Source: ESET poll of 488 MSP partners in 14 countries during July 2019, via an online questionnaire.

On Android devices additional computational load causes:

- Shorter battery life
- Noticeably increased device temperature
- Lower device productivity
- In worst-case scenarios, physical damage to the battery from "bloating"

Keep your IT infrastructure free of cryptominers

- Protect endpoints, servers and other devices by implementing **reliable and multilayered security solutions** that are able to detect potentially unwanted (PUA) cryptomining scripts as well as cryptomining Trojans

- Implement **Intrusion Detection Software (IDS)** that helps identify suspicious network patterns and communications potentially tied to illicit cryptomining (e.g. infected domains, outgoing connections on typical mining ports such as 3333, 4444 or 8333, signs of persistence, etc.)

- **Increase network visibility** by using a remote management console to enforce security policies, monitor system status, and secure company endpoints and servers

- **Train all employees** (including senior management and network administrators) in how to maintain good cyber-hygiene and create and use strong passwords, reinforced with multi-factor authentication, thus increasing the protection of company systems in case passwords are leaked or brute-forced

- Follow the **principle of least privilege**. All users should have user accounts with the minimum permissions need to allow them to complete their current tasks. This approach significantly lowers the risk of users and admins being manipulated into opening or installing cryptominers or other malicious software in a device connected to the company network

- Use **application controls** that reduce to a minimum the software allowed to run, preventing the installation of cryptomining malware

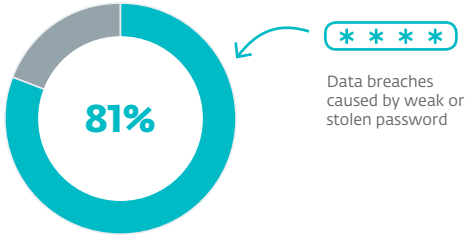
- Implement a **good** update and patching policy to significantly lower the chance of an organization being compromised via previously-known vulnerabilities; many advanced cryptominers use known exploits, such as EternalBlue, for their primary distribution

- **Monitor** company systems for **excessive power usage** or other energy consumption anomalies that might point to unsolicited cryptomining activity.

4 Password security
What's at stake?

Passwords are a basic security measure, yet their growing number and complexity makes them challenging to manage and use safely. That's why additional protective solutions, such as multi-factor authentication (MFA), are necessary to strengthen password access.

SMBs are a sweet spot for cybercriminals, as they have more valuable data and assets than consumers, and they are more vulnerable than enterprises, which have larger security budgets. This problem is amplified by the growing number of businesses incorporating "smart" devices into their IT infrastructure. While the Internet of Things (IoT) helps them to make business operations faster and smoother, these devices are often vulnerable and run with publicly available default admin usernames and passwords, posing a risk that can lead to harmful consequences.



According to the Verizon 2017 Data Breach Investigations Report, as many as **81% of data breaches were caused by weak or stolen passwords.** Given that more than 5 billion passwords have been leaked online, basic password protection is being rendered ineffective.

Poor password security implications

The EU's General Data Protection Regulation (GDPR) states that **organizations of all sizes must ensure the security of the data they hold** by implementing "appropriate technical and organizational measures". So if a breach occurs, and only simple and static passwords are in place, a large fine is possible.

Ways to improve your password protection

Implement effective password policies. Employees need to be trained in how to create strong passwords

8 steps to create strong passwords

Your IT department should implement rules when setting and enforcing company password policy

6 basic rules for a good password policy

To better protect data, employ multi-factor authentication (MFA)

ESET Secure Authentication

Even stronger protection

As SMS and mobile devices are frequently subject to malware attacks, modern MFA solutions tend to use push notifications, which are more secure as well as user-friendly, rather than SMS verification. To further increase the security of the authentication process, organizations can add **biometry** — *something the user is* — to augment access protection.

OVERCOME
THE TOP SECURITY CHALLENGES FOR SMBS

Tackle ransomware, combat social engineering, stop illicit cryptomining and strengthen password security.

HOW ESET CAN HELP

ESET, North America
610 W. Ash Street, Suite #1700
San Diego, CA 92101

partnerservices@eset.com
(619) 876-5489
https://www.eset.com/us/

CYBERSECURITY EXPERTS ON YOUR SIDE