The employee cyber-security handbook

Your go-to guide for security tips and intel

Table of contents

Your role in cybersecurity 3
- Social engineering 4
- Common social engineering techniques 5
- Malware 6

Follow cybersecurity best practices 7
- Choose a password strong enough to resist an attack 7
- Use multi-factor authentication 8
- When you receive an email, take time to inspect it 8
- Don't click on suspicious hyperlinks or attachments 9
- Be aware of the risks associated with modern work tools 9
- Patch early, update often 10
- Build a security-first culture 10

Conclusion 11

Your printable cybersecurity checklist 12

Your role in cybersecurity

From the CEO to the newest hire, cybersecurity is a responsibility for everyone in the company—not just the IT team. There are a few reasons why.

The first is that there are more opportunities than ever for an attack. Threat surfaces have increased in size—every device or account you use represents a potential area of attack.

Second, the tools needed to launch an attack have become more accessible than ever, thanks to the growth in cybercrime-as-a-service markets. Anyone with ill intent and a few dollars to spare can access the software necessary to stage an attack.

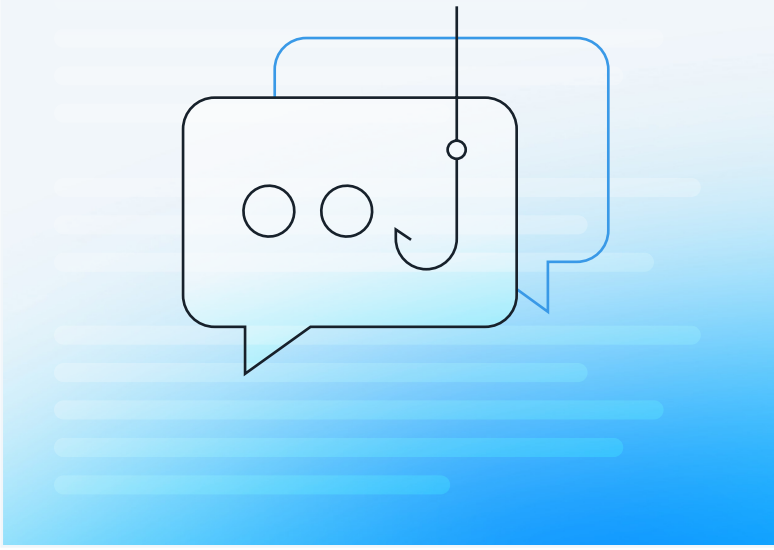
Additionally, cybercriminals are also taking advantage of the efficiencies and advancements brought to us by new AI tools and technologies.

Third, people are often the weakest link in cybersecurity. Despite organizations spending billions[1] on security measures each year, attacks still happen. People make mistakes, and attackers capitalize on this.

But the thing is: knowledge truly is power. This handbook holds all the critical information you need to know about cyberattacks—including the techniques and tactics adversaries use—and best practices to stop threat actors in their tracks.

Social engineering

At its core, social engineering is manipulation.



An attacker may use a social engineering scam to trick you into launching malicious software. Or they may convince you to voluntarily provide usernames and passwords, private client data, confidential business files, or the company's financial details.

We'll cover three very common social engineering attacks to be aware of: phishing, spear phishing, and business email compromise (BEC).

Phishing

Phishing refers to a type of cyberattack usually delivered as an email, used to obtain sensitive information or data such as bank account numbers or passwords.

It's important to note, however, that while email-based phishing is the most well-known, threat actors also use text messages (smishing) and voice calls (vishing) for their attacks.

Cybercriminals engineer these messages before broadly and randomly sending them out to trick recipients into performing an action that furthers the attack. They're casting a wide net to catch as many fish as possible—or should that be phish?

Spear phishing

Spear phishing, meanwhile, operates on similar principles, but instead of focusing on catching as many victims as possible, attackers will tailor highly targeted messages to a single victim. As a result, spear phishing generally takes more time and effort to implement, but can have more significant impacts.

Business email compromise

Finally, business email compromise (BEC), sometimes known as CEO fraud, takes both phishing and spear phishing techniques and puts them to use to exploit an employee's sense of urgency.

Once they're ready, the attacker will send a carefully crafted message to an employee, usually late in the workday or after hours, with some urgent request to initiate a financial transfer. The message relies on employees not thinking twice about the last-minute message to help a boss out. In a moment of distraction, it's entirely possible an employee could fall for such a message and inadvertently wire transfer funds to an attacker-controlled account.

In other instances, the attacker may pose as the financial department of a business and send out phony invoices, but not before setting up email forwarding rules to keep their activities hidden.

Email hijacking can make these types of attacks particularly difficult to spot. In email hijacking, the cybercriminal has control of one of the accounts in an email conversation and uses the thread's information to craft their lure. On top of that, the email comes from a real, trusted person, circumventing many technical precautions.

Common social engineering techniques

AI tooling has made crafting message lures easier. Threat actors can feed all the relevant information into their tool of choice and, within seconds, have believable messaging in any language they wish.

But whether they use AI or not, cybercriminals still rely on a few key techniques for their social engineering scams. Let's dig into some of the specific techniques used in social engineering scams:

They impersonate authority figures or someone you trust

As we've already briefly touched on, attackers will often pose as a high-ranking executive you know and trust, such as the CEO. Disguised as someone else, the attacker may ask you to send a wire transfer, company credentials, or other confidential information.

This technique is effective for two main reasons:

- You're more likely to open an email from your CEO than a stranger.
- You're less likely to question a request from an authority figure.

EXAMPLE:
You receive a seemingly urgent email from your manager, the CFO. She's stuck in a meeting that's running late and needs you to issue a payment to a new vendor with all the key financial information to do so. Unfortunately, the email isn't really from your CFO and that "new vendor" is actually a threat actor's banking account.

They prey on your need for information

In phishing attacks, attackers may encourage you to open their email by falsely offering new information. The attacker purposefully designs the scam to pique your curiosity, as you may be more likely to open files or links to gain that information.

EXAMPLE:
You receive an email from what looks like your bank, offering information about new interest rates. It could impact your finances, so you open the file. But it's malware, and you've unknowingly granted the attacker access to your device.

They use fear or urgency to pressure you to act

Attackers design phishing campaigns using limited time offers or with tasks requiring urgent action. Despite knowing better than to open a link without first inspecting it, you may follow directions haphazardly if you feel pressured to act quickly.

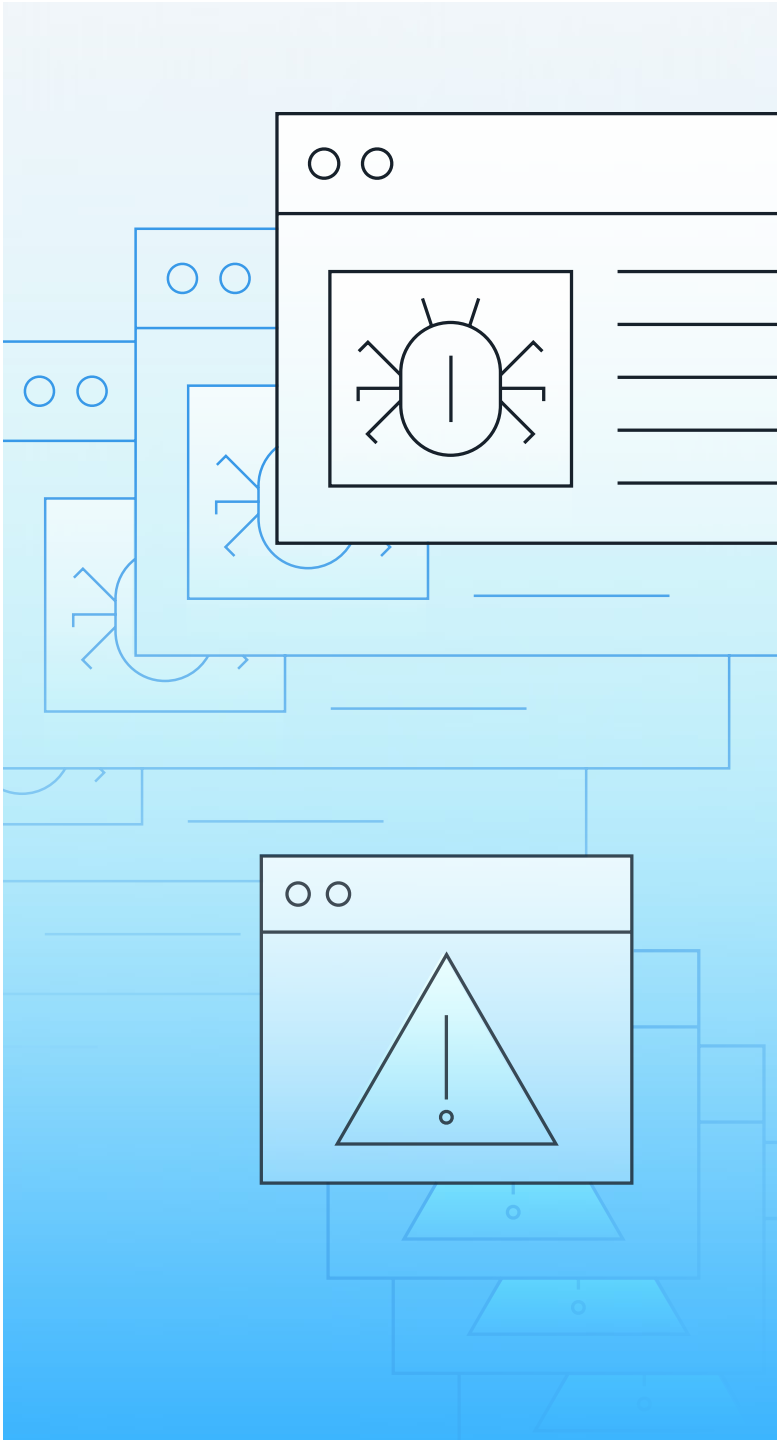
EXAMPLE:
You receive an email, seemingly from a recognized brand, offering $1000 to the first ten people who sign up for their newsletter. You register, willingly giving the attacker key personal information, as well as banking information for where they should send that $1000.

They hide their attack among the noise of current events

Attackers know that governments, suppliers, businesses, families, and friends send information related to current events. Organizations often use consistent email formats, webpage layouts, and messaging that attackers can then copy and use in their malicious versions.

EXAMPLE:
It's tax season, and you receive an email from what appears to be your finance department. They're sending you a PDF that outlines what they need to file taxes for the company on time.

The document is malicious, but because you're expecting something tax-related, you click anyway.



Malware

Malware has become ubiquitous in cybersecurity. And while it's difficult for those less-technical to know if malware infected their system, anyone can improve their cyber defenses by recognizing how it's delivered.

The most common method? Phishing emails, trojans (a type of malware disguised as a genuine program but can actually perform harmful actions) and malvertising (the use of online advertising to distribute malware).

Once on your device, malware lets the attacker carry out unauthorized actions. They may take over your financial accounts, lock down your systems, compromise and steal sensitive personal or company data, cause reputation damage, or even disrupt entire operations.

Ransomware[2] similarly prevents you from accessing data, files, and systems. Ransomware, however, encrypts files using a key controlled by the attacker, blocking access until a predetermined sum is paid.

Follow cybersecurity best practices

Modern work requires you to use email, cloud applications, and the Internet—all of which add security risks. That's why following best computing practices is critical, no matter the size of the company you work for, where you work from, or the type of work that you do.

Choose passwords strong enough to resist an attack

The most critical security rule? Never reuse passwords across different accounts.

It's important you use unique and hard-to-guess[3] passwords to keep attackers out, because 70% of the most common passwords can be cracked in about 70 seconds.[4]

Thankfully, there are a couple easy ways to create complex passwords:

01 Use passphrases. A passphrase is a sequence of words that makes sense to you and no one else, such as BlackBookcaseSpiderPlant. Why does this technique work? It's much easier to remember a few words[5] that make sense to you than it is to remember 12+ randomized characters.

02 Use a password manager[6] to create, store, and retrieve distinctive passwords for your accounts. Most password manager tools can autogenerate complex strings of letters, numbers, and symbols, so you can create unique passwords for each account without having to remember them all.

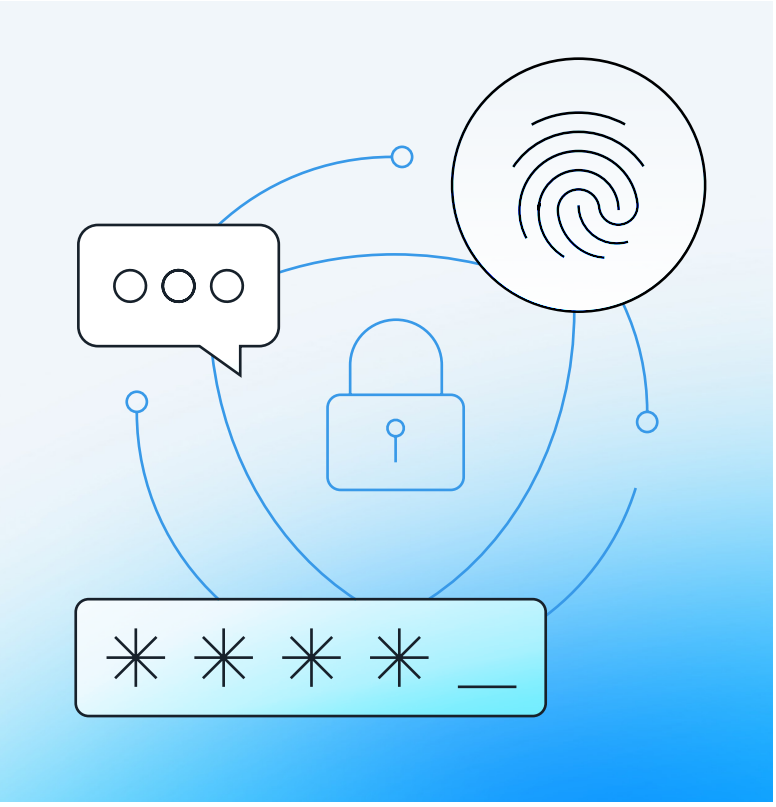
No matter which method you use, here are a few more password-related tips to keep in mind:

- Avoid using personal information in your passwords, such as your name, date of birth, or place of work.
- Avoid typical replacement characters, such as the "@" symbol in place of the letter "a."
- Avoid using passphrases that have any meaning to others.
- Never share your passwords with anyone.
- Avoid enabling the "Show my Password" feature while logging in to your accounts—especially if you're in a public space.

Use multi-factor authentication

Multi-factor authentication (MFA) adds another layer of cybersecurity. MFA can help protect against a number of common cyberattacks, including:

- Credential stuffing—using previously compromised account credentials to gain access.
- Brute force—systematically guessing all possible username and password combinations until successful.



When you receive an email, take time to inspect it

Avoid complacency in your email routine. Be wary of email senders masking their true identity. Like a pickpocket, attackers employ distraction techniques to obscure their scheme.

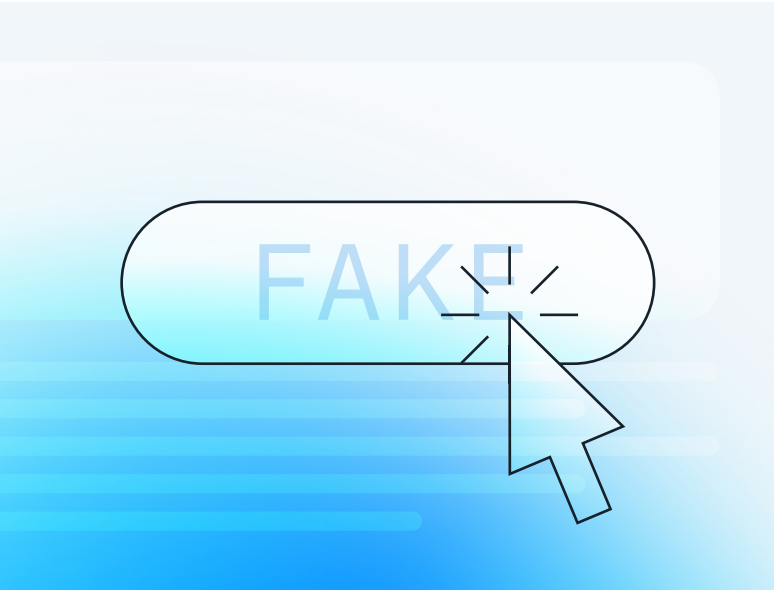
Pause to inspect the sender's email address and display name more closely, especially if they are asking you to do something, such as login to a website, send sensitive files, or transfer money. If you have doubts, use another method to contact the sender—by phone or in person—to ask if they sent the email.

Here are two common schemes to watch for:

- Attackers posing as someone else—often a person you know and trust—may use that person's full name (John Smith) or legitimate email address (johnsmith@xyz.com) as their display name. This is called "spoofing" and makes it appear as though the email is coming from the right person.
- Attackers may also use homoglyphs—any identical or similar-looking text characters—to look like the intended sender's email address. A familiar example of this scheme in action is replacing a capital letter "O" with a zero.

Even if the sender's email address seems real, the attacker may have accessed the account of a legitimate user and sent the message as part of a business email compromise attack.[7]

If your company uses Field Effect MDR,[8] you can forward the email to our team of cyber experts via the integrated Suspicious Email Analysis Service (SEAS). We'll inspect the message right away and let you know step-by-step how to deal with the email.



Don't click on suspicious hyperlinks or attachments

If you receive a suspicious phishing email, don't click on any links or open any files. Clicking on any part of the email could lead you to download malware or to a login page that appears authentic, but entering your credentials exposes them to the attacker.

At a minimum, clicking on a suspicious link might let the attacker know that you received and opened their email. This establishes communication between your system and the attacker and may enable the subsequent attack.

Our team at Field Effect has found that attackers are increasingly using clickable images and QR codes in their attacks. By using an image or QR code instead of text, the attacker can still link to a malicious website, all while evading any text filters in place to keep them out.

A TIP FROM THE EXPERTS:
Following an email link may lead you to a website that looks real but is not. Instead, bookmark websites you frequent—especially those requiring your credentials such as online banking—and use the bookmark to access the page instead of the hyperlink in the email.

Be aware of the risks associated with modern work tools

As we rely on video conferencing software, messaging apps, and cloud-based services to enable remote work, we must consider the new opportunities they present for attackers.

Here are just a few of the risks that come with these tools:

- Logging in from home (or other locations) presents a new opportunity for hackers to remotely access systems.
- Using improperly configured tools, apps, and services allow hackers the chance to abuse these misconfigurations.
- These technologies have new vulnerabilities uncovered every day that are then shared online with others.

Securing against these cyber threats requires effort from all parties. IT should configure devices and accounts properly, provide reliable tools for remote access, and implement a powerful threat monitoring, detection, and response solution.[9]

Your role, however, is equally important. Human error continues to be a leading cause of data breaches,[10] so you must be aware of the security risks and diligent while using these tools.

Patch early, update often

Keeping your software and systems updated is another one of cybersecurity's golden rules. Vendors frequently release new versions of their software to add features, improve performance, and fix security vulnerabilities. Failure to install updates in a timely manner may be leaving your digital doors open to intruders.

Consider that every piece of software in your organization—from your computer's operating system to your smartphone apps—constitutes a potential entry point for cybercriminals. That can add up to a lot of entry points.

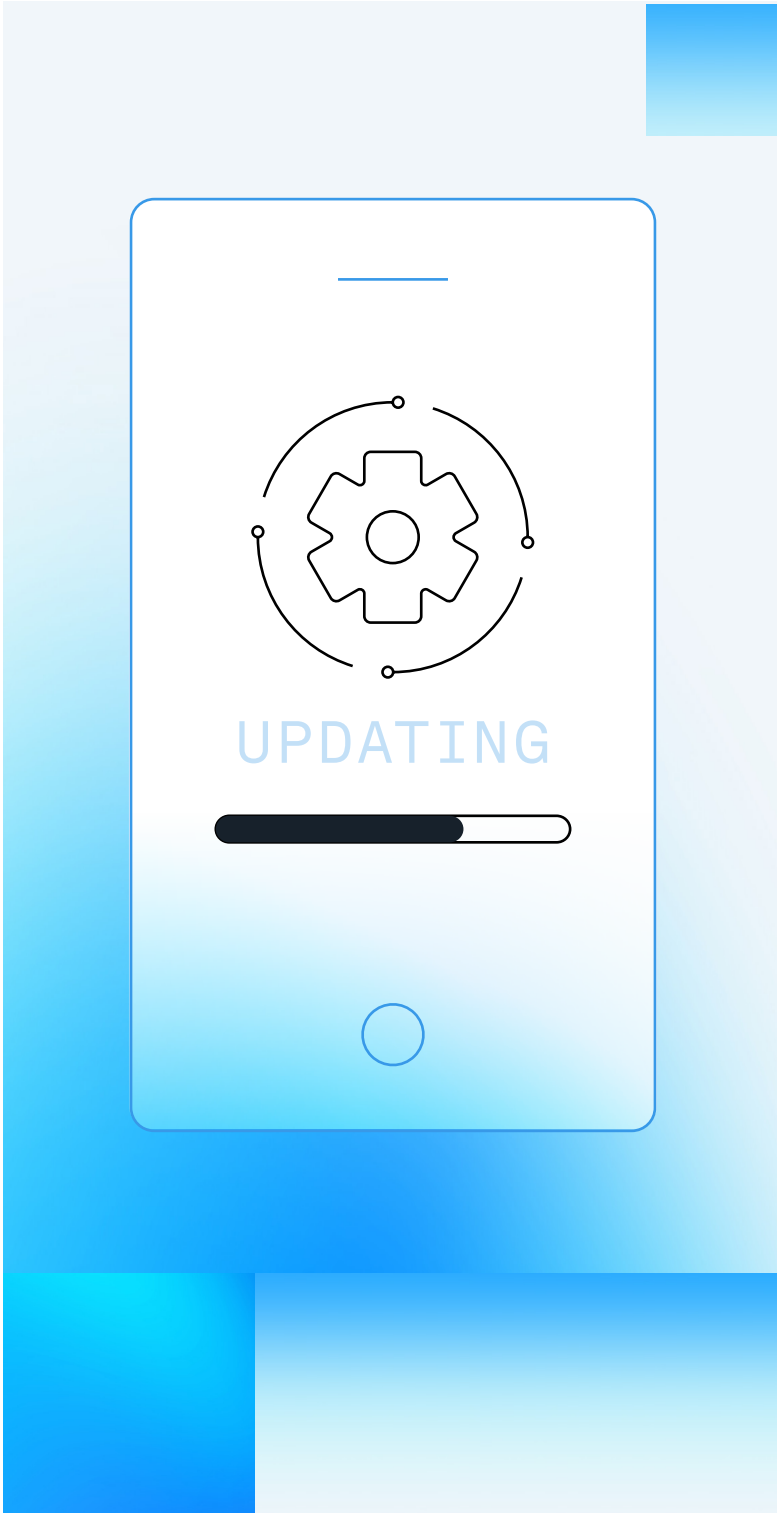
Build a security-first culture

Cybersecurity cannot be a check-the-box activity; it needs to be an ongoing commitment. Ensure this by integrating security as a company value and as part of the culture.

Everyone in the company has a role to play and a responsibility to build a safer, more secure workplace. Here are a few ways to do that:

- Be a security champion in your organization.
- Stay up to date on threats and techniques.
- Follow cybersecurity regulations and policies.
- Demonstrate security best practices for others.
- Avoid complacency while conducting business using technology.

A security-first culture keeps cyber threats top of mind and enables you, as an employee, to contribute actively to the safety of your business.

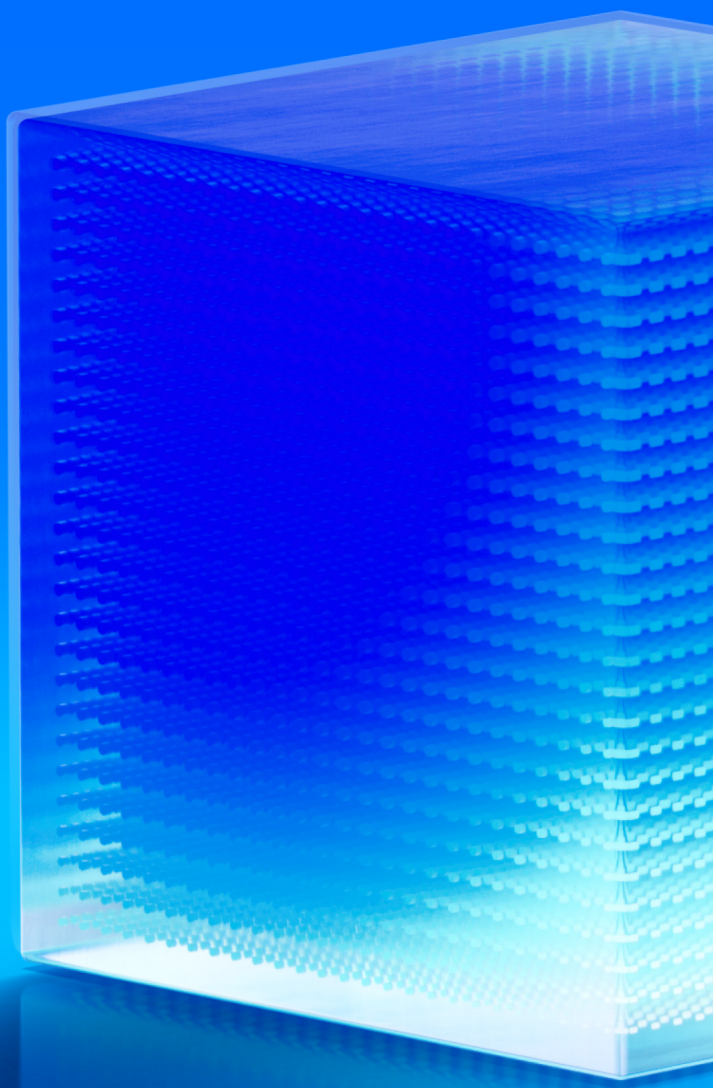


Conclusion

While it's extremely important to have cyber insurance and backups, you can't rely on these things to prevent an attack. By proactively encouraging cybersecurity responsibility across the entire company, you can help to avoid threats altogether.

Remember, you're not alone. It's our mission to help protect small and mid-size businesses. If you have any questions, or need any help with your cybersecurity, get in touch with our Field Effect team.

We've got your back.



SOURCES

1. https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024#:~:text=Worldwide%20end%2Duser%20spending%20on,estimated%20to%20reach%20%24188.1%20billion.
2. https://fieldeffect.com/blog/what-small-businesses-need-to-know-about-ransomware/
3. https://fieldeffect.com/blog/why-use-a-password-manager/
4. https://globalnews.ca/news/10094300/canada-bad-passwords-top-20-list/#
5. https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd
6. https://fieldeffect.com/blog/why-use-a-password-manager/
7. https://fieldeffect.com/blog/how-to-spot-business-email-compromise-attack/
8. https://fieldeffect.com/products/covalence-cyber-security/
9. https://fieldeffect.com/products/covalence-cyber-security/
10. https://www.industryweek.com/technology-and-iiot/article/21131736/verizon-dbir-we-have-a-people-problem

Your printable cybersecurity checklist

Cybersecurity is critical to the success of the company; defending against modern threats is everyone's responsibility. The good news is you don't need to be an expert with years of security experience to help protect yourself and your organization.

Print out this checklist and hang it up in your office—whether that's at home or work. Let it be a reminder of your role in keeping the company safe and a test to ensure you're still following cybersecurity best practices!

Phishing techniques to watch out for:

- [ ] Impersonating an authority figure or someone you know and trust
- [ ] Preying on your need for information
- [ ] Using fear or urgency to pressure you to act
- [ ] Hiding their attack among the noise of current events

Best practices for creating and managing passwords.

- [ ] Use passphrases and/or a password manager
- [ ] Avoid using personal information in your passwords, such as your name, date of birth, or place of work
- [ ] Avoid typical replacement characters, such as the "@" symbol in place of the letter "a"
- [ ] Never reuse passwords across different accounts.
- [ ] Avoid using passphrases that have any meaning to others
- [ ] Never share your passwords with anyone
- [ ] Avoid enabling the "Show my Password" feature while logging in to your accounts – especially if you're in a public space

Other cybersecurity best practices to remember:

- [ ] Use multi-factor authentication
- [ ] Take the time to inspect emails
- [ ] Don't click on suspicious links or attachments
- [ ] Always consider the risks of remote work tools
- [ ] Be a security champion in your organization
- [ ] Stay up to date on threats and techniques*

* visit www.fieldeffect.com/blog to learn more

We're on a mission to protect small and mid-size businesses.
If you have any questions, or need any help with your cybersecurity, reach out!

Profound simplicity, powerful cybersecurity.

Field Effect MDR is an advanced cybersecurity solution that monitors and protects your entire threat surface—endpoints, networks, and cloud services—all from a single platform. No add-ons, no modules, and no gaps in your security. Field Effect MDR not only monitors every aspect of a business's threat surface, but reduces alert fatigue and false positives by aggregating data from multiple security events into simple, actionable remediation steps.

FIELD EFFECT / MDR

About Field Effect

Field Effect believes that businesses of all sizes deserve powerful cybersecurity solution.

Our threat detection, monitoring, training, and compliance products and services are the result of years of research and development by the brightest talents in the cybersecurity industry. Our solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:

CANADA + UNITED STATES
+1 (800) 299-8986

UNITED KINGDOM
+44 (0) 800 086 9176

AUSTRALIA
+61 1800 431418