Basic Cyber Hygiene Practices That Go A Long Way

Doros Hadjizenonos, regional sales director at Fortinet in South Africa

When on the job at a corporate office, a healthcare organization, or an academic institution or government agency, or even when you are working from a local coffee shop, restaurant, or home office, your organization's online safety and security is a responsibility shared by all. However, as mobile computing—especially using personal devices—becomes more common, the potential for network compromise is increasing.

Think about this: around the world, 20 percent of employees now do some or all of their work from home. Employees increasingly demand flexible and seamless enterprise access, making mobility a top global priority in order to attract talent and provide competitive advantages. While this trend gives employees increased access to the network without tying them to a cubicle, it also introduces new security risks to the organization.

As mobility and digital transformation demands have made business networks more accessible than ever, cyberattacks are also becoming more frequent and sophisticated, taking advantage of the expanded attack surface. As a result, employees can unwittingly cause severe damage to a business due to a lack of cybersecurity awareness. A compromised device or an unreliable remote connection can leave your network vulnerable.

To minimize risk as work and home, especially as connectivity and digital resources become more intertwined, organizations need to promote security hygiene best practices that will minimize risk, data leakage, and non-compliance while still allowing for operational flexibility and efficiency.

Building a Culture of Strong Cyber Hygiene

As we use our own devices to remotely connect to the corporate network, we must all play a role in helping to keep the network secure. Here are a few strategies that everyone can practice to promote top-notch cyber hygiene.

1 **Use Secure Access Points & Create a Work Network**

When remotely connecting to your corporate network, cyber hygiene best practices recommend using a secure access point. One way to minimize the risks of connecting to your work network over public Wi-Fi is to use a virtual private network (VPN). VPNs allow you to extend your private network across the public Wi-Fi using an encrypted virtual point-to-point connection which enables and maintains secure access to corporate resources. However, it is still critical to remember that if either end of that VPN is compromised, like the unadvertised WiFi access point at your local coffeeshop, then VPN cannot prevent things like man-in-the-middle attacks. This is why it is also imperative that you ensure the integrity of any access point you connect to. While public Wi-Fi connections are often harmless, it only takes one malicious connection for a cybercriminal to intercept all of your browsing data as you move across sites and accounts.

Another best practice is to create a secure network for business transactions in your home office. Most businesses have two separate networks– one that only employees can access and one for guests. This same protocol is easy to replicate at home. Most home routers allow for the creation of multiple networks, such as a home and a guest connection. Adding a password protected network for work connections means that your corporate resources will never share the same connection as your gaming systems, home laptops, your children's smart devices. By keeping your home devices separated from the network on which you access sensitive work data, compromised devices or applications cannot be used as an point of vulnerability to attack the corporate network.

2 **Update Regularly**

Installing updates across devices, applications, and operating systems on a regular basis is an integral step to achieving strong cyber hygiene. Though it's easy to ignore updates when you need to meet a deadline or help a customer, failure to keep your devices updated can drastically simplify the process for cybercriminals seeking to corrupt your device. One of the most effective—and easiest—ways to avoid that tendency is to simply add patching and updating to your work schedule. It's hard to fit something in if it's not on your calendar for the day. If you don't schedule it like you do other

tasks and meetings, it's easy to push it to another day.
Regularly applying updates and patches ensures that the operating system and applications you are using are protected against known vulnerabilities. One recent attack that demonstrates the importance of these updates is WannaCry, which leveraged known Microsoft vulnerabilities—for which patches were readily available—to distribute ransomware. Had the targeted organizations and remote end users simply administered updates and patches to their devices they would have been far less susceptible to this attack.
In this same vein, it's also important to ensure all of the programs and applications that run within the business network are still supported by the publisher, and that you retire or replace those that are not.

3 **Strong Access Management**

Access management is a simple but very effective cyber hygiene best practice. You should be using strong passwords and two-factor authentication across all devices and accounts.
Passwords should be complex, incorporating numbers and special characters. And try to avoid reusing passwords across accounts – especially on devices and applications that are used to access sensitive business information. This is because if your account is breached on one site, and your information is leaked, credential stuffing and brute force attacks can use this leaked information to target other accounts.
The biggest challenge for this sort of password strategy is simply remembering or keeping track of them. Because of this, many of the stronger passwords are actually easier to guess. Instead, use acronyms or phrases to help with remembering passwords. And as the number of passwords you need to remember increases, consider employing management software to help you keep track of them.
Strong passwords augmented with two-factor authentication is even better, ensuring that only authorized people can access business-critical systems and sensitive data. Recent advances in biometrics, such as fingerprint scanners and facial recognition software, provide similar multi-factor authentication. Additionally, use segmentation, network admission control, and role-based access controls to limit the users and devices that can access high-value, sensitive information.

4 **Practice Safe Email Use**

The most popular attack vector still being leveraged by cybercriminals today is email. Because of its uniquitous use, it remains the easiest way to distribute malware to unsuspecting users. Though there are many ways cybercriminals leverage email for malicious activities, ultimately, they largely rely on tricking recipients into clicking on malicious links and attachments, often by impersonating another employee or someone they know.
Some of the most popular email scams are phishing and spear phishing. Phishing attacks include links to websites that look legitimate, such as a bank, business, or government office, which then ask users to log in—thereby stealing credentials or infecting the device with malware. Spear phishing increases the effectiveness of such attacks by impersonating an employee or trusted user before requesting login information, sensitive employee data, money transfers, or simply asking them to open an infected attachment or click on a malicious link.
To combat such threats, you must be vigilant when responding to emails, especially those with links and attachments. Never click on a link or attachment from an unknown sender. And even if an email seems to come from a trusted source, be sure to look closely lat the email address or website URL they refer you to. Often, names or URLs will have misspellings, which indicate an attack. Even if things look normal, stop and ask yourself if this looks or sounds like something this person would send to you or ask you to do. Most of the time, links are only provided after a request has been made, or as part of a larger or longer conversation. Unexpected requests are ALWAYS suspect, and may warrant directly contacting the sender to not only verify the request, but if it is legitimate, to also suggest that they use a different process besides distributing unannounced attachments and links.

5 **Install Anti-Malware**

While anti-malware software cannot stop unknown attacks, the vast majority of attacks and exploits reuse attacks that have been previously successful. Installing anti-malware/anti-virus software across all your devices and networks provides protection in the event of a successful phishing scam or an attempt to exploit a known vulnerability. In addition, look for tools that provide sandboxing functionality, whether as part of an installed security package or as a cloud-based service, to also detect Zero-Day and other unknown threats.

6 **Have a Cyber Response Plan in Place and Understand the Details**

All businesses, regardless of size, should have an incident response and recovery plan in place to minimize downtime in the event of an attack. Make sure you and all other employees are aware of this plan so there are no questions about the next steps during an attack. This includes having a hotline prominently displayed so employees know who to contact if they suspect there has been a breach. You also need to ensure that this hotline is either manned 24/7 or that an after-hours number is readily available. Waiting to learn about a breach until after your support team arrives for work may be too late.

Having a streamlined plan combined with a staff that are all on the same page will allow you and your business to quickly stop an attack from spreading throughout the network, reduce dwell time, minimize the exfiltration of data, and get everyone back online faster.

Final Thoughts

Cybersecurity is no longer the sole responsibility of the IT and security teams. As employees interact with and rely on technology every day, often from remote locations, they all play an integral role in the security of the organization.

In order to ensure security and compliance, especially as trends such as digital transformation and mobility continue to expand, each individual employee must understand and practice cyber hygiene. By being aware of common attack vectors and utilizing the tips provided above, your users can help stop the spread of malware and keep your business running smoothly.