Cracking the Hackers: How to Build a 100% Engaged Human Firewall

Critical steps for a successful cyber security awareness campaign

The Cyber Threat Today

Every day over 2,200 cyber-attacks hit organizations around the world. That's one attack every 39 seconds.[1]

And the risk is rising. Cyber criminals are exploiting business operations already strained by COVID-related disruption.

Many companies were not prepared for increased cyber-attacks. Some have still not recovered.

> **"The pandemic has highlighted vulnerabilities and accelerated the understanding of the cyber warfare space."**
>
> – Tracy Reinhold, VP and Chief Security Officer, Everbridge

Staff working remotely are at greater risk of compromising organizational security. Home connections are less secure. Employees are distracted. Cyber criminals have an easier entry into the company network.

The human firewall is under threat. Phishing scams, malware and other tactics exploit remote workers' weaknesses. Research shows that 43% of employees have made mistakes that could have resulted in cyber security attacks.[2]

Doubling down and ensuring 100% effectiveness of your human firewall has never been more important.

Cyber-crime increased

273%

in the first half of 2020 compared with the same time in 2019.[3]

Adopting a Block and Tackle Strategy

Cyber-attacks have many objectives. Theft, corporate espionage, destabilization, political agendas or simple mischief.

While technological solutions and processes provide part of the solution, new technologies for cyber-attacks have evolved as well. Rapid IT changes are a top cyber security challenge. Technology alone isn't protection enough.

A robust security profile requires a strong defense against current threats, and proactively arming the organization against possible future threats. It's what Tracy Reinhold, Vice President and Chief Security Officer at Everbridge, calls blocking and tackling.

90% of all cyber security attacks begin with human error.[4]

Communications are critical in a block and tackle strategy. Security must be built into the fabric of the company culture as an all-hands, no exceptions business approach.

Staff must be aware of safe practices to follow, understand the real harm that breaches have caused other companies, and repeatedly reminded to comply. Emerging threats must be socialized to minimize the risk of exposure from employee errors as more detail becomes known.

Knowledge delivered through effective communications, leads to safe, secure behavior – and an effective human firewall which protects devices, networks, individuals and the organization.

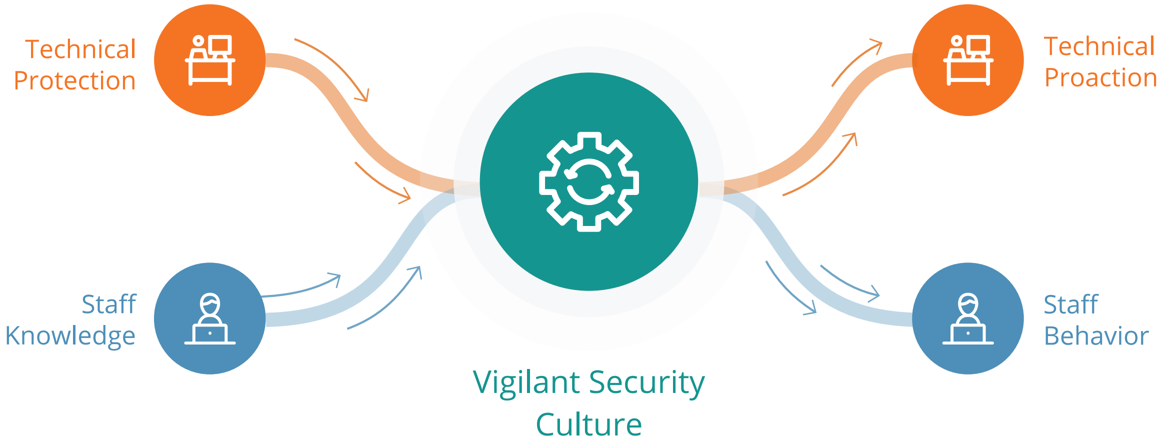
> **"By blocking and tackling I mean, are you doing your patching, are you updating your software, are you installing your antivirus software. All of this sounds really straightforward, but it's amazing how many companies don't do it. By doing the basics you you're making it more difficult for threat actors to access your system."**
>
> – Tracy Reinhold, VP and Chief Security Officer, Everbridge

Effective communication overcomes misinformation. It establishes cyber security as a serious issue with real risks and consequences– not a theoretical threat that employees need not take seriously.

It also protects an organization's reputation externally, particularly if a security breach occurs that affects uptime, customer service, data compromise, or trust in general.

Forcepoint found that only 46% of leaders regularly review their cyber security strategies.[5] But without the right employee communications, business protection will always be compromised. Correct cyber security values and behaviors have to become ingrained to effectively mitigate the risks.

The threats have evolved – your communications need to as well.



Business technology which provides fundamental protection and the ability to scale proactively

Staff communications which build workforce knowledge and improve correct behaviors

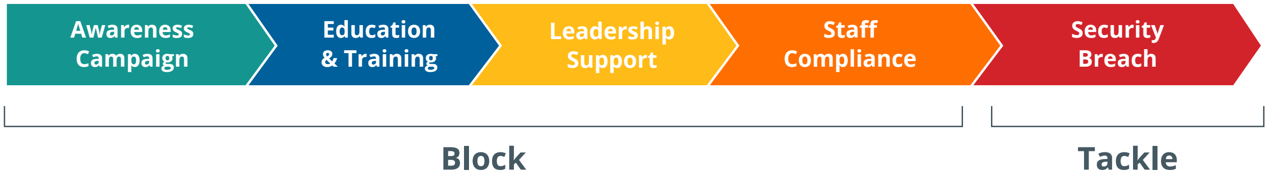
> **"Previously, it was all about the technology. You installed antivirus software and put in firewalls. That's still very, very important, but it doesn't help you if staff click on a link that downloads a piece of malicious software."**
>
> – Angela Henry, Information Security Operations Head, South African bank

> **"Today the speed of communications is so fast that if you don't control the narrative, the narrative will control you. While you have to address the problem from a technical perspective, if you don't get ahead of the threat and inform your stakeholders and customers, then you are at the mercy of social media or anybody else."**
>
> – Tracy Reinhold, VP and Chief Security Officer, Everbridge

From Training to Breaches: Resolving InfoSec Needs

Strong human firewalls mean businesses can guard themselves against ever-evolving cyber threats.

Communications are critical – before, during and after a cyber security incident. Information Security Managers must use a range of communication tactics to maximize the knowledge and behaviors of staff.


Awareness Campaign

Education & Training

Leadership Support

Staff Compliance

Security Breach

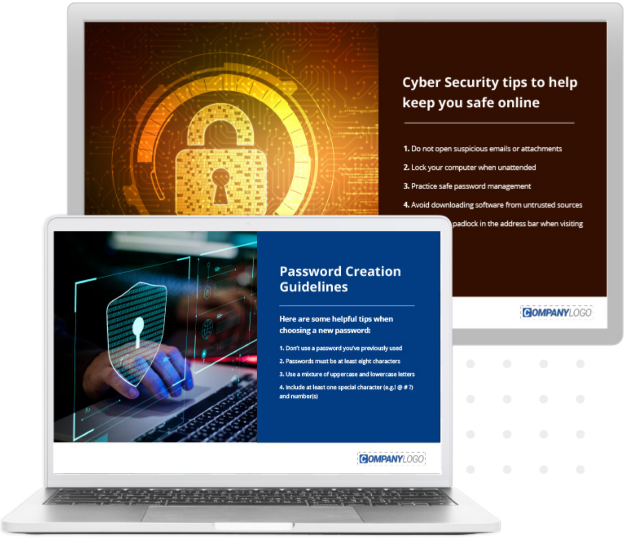
Block

Tackle

Awareness Campaigns

Cyber security promotion can't be a 'one and done' exercise. Employees need repeated exposure to information, and a combination of complimentary communication channels in order to absorb it. Reinforcement of key messages is essential for them to be read, understood, and acted upon.

Action: Use corporate screensavers in your InfoSec awareness campaigns to turn idle computer screens into powerful promotional tools. Remind staff of steps to follow in a phishing attack, direct them to your intranet for latest information and policies, and reinforce that cyber security is everyone's responsibility.


Cyber Security tips to help keep you safe online

1. Do not open suspicious emails or attachments
2. Lock your computer when unattended
3. Practice safe password management
4. Avoid downloading software from untrusted sources

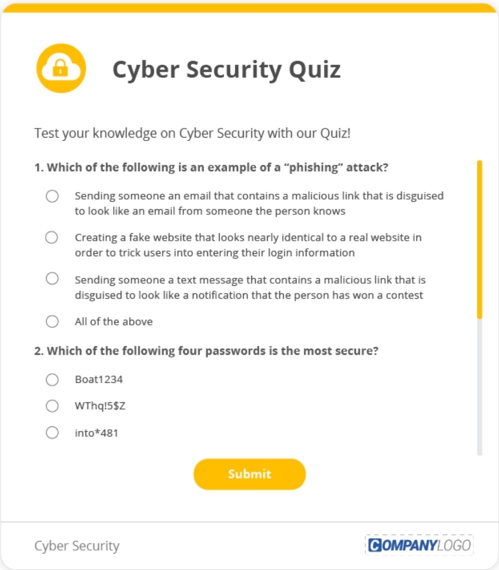
padlock in the address bar when visiting

Password Creation Guidelines

Here are some helpful tips when choosing a new password:

1. Don't use a password you've previously used
2. Passwords must be at least eight characters
3. Use a mixture of uppercase and lowercase letters
4. Include at least one special character (e.g.! @ # ?) and number(s)

> "With the way that we work today, we mix our personal and our business lives, sometimes on the same machines. This leads to vulnerability in your private life, so that brings in the duty of care for an organization. I find that it's duty to care and not duty of care. We have to educate our workforce about cyber security, about the machines that we use and how to protect them."
>
> – Tracy Reinhold, VP and Chief Security Officer, Everbridge



Cyber Security Quiz

Test your knowledge on Cyber Security with our Quiz!

1. Which of the following is an example of a "phishing" attack?

○ Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows

○ Creating a fake website that looks nearly identical to a real website in order to trick users into entering their login information

○ Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest

○ All of the above

2. Which of the following four passwords is the most secure?

○ Boat1234

○ WThq!5$Z

○ into*481

Education and Training

Regular training should keep employees abreast of emerging cyber security threats and examples of security failures. Tailor training to simulate the unique threats that different teams face so that scenarios are more relatable and relevant to them. Conduct interactive attack simulations to provide employees with hands-on experience they can recall when they need to react quickly.

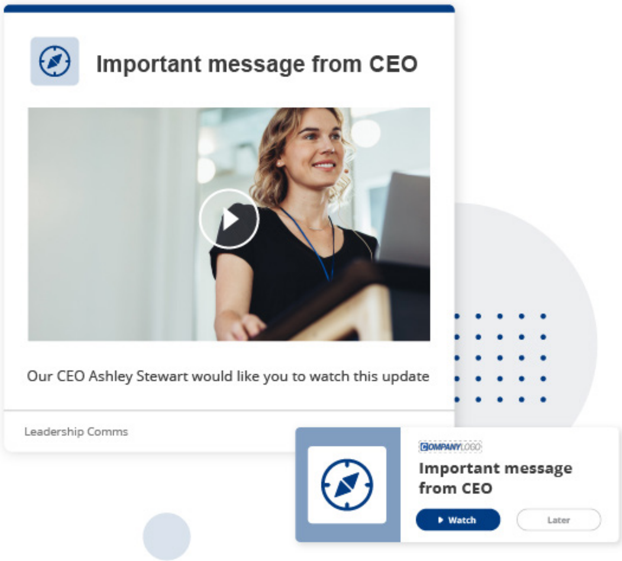
Action: Assess the effectiveness of training sessions through online quizzes. Test employees on what they've learned. This identifies knowledge gaps where further training are required.

> **"User education is one of the top things you've got to get right to protect yourself."**
>
> – Service Operations Manager, Major UK healthcare provider

Leadership Support

Leaders' sponsorship and voices are essential in building security into the fabric of the company culture. They model the ideal behavior for an organization and elevate its importance among business priorities, including highlighting the consequences of non-compliance by individuals. Employees look to leadership to set the benchmark in prioritizing cyber risk management.

Action: Feature leadership in video messages to communicate desired behaviors and reinforce the importance of the issue throughout the organization.

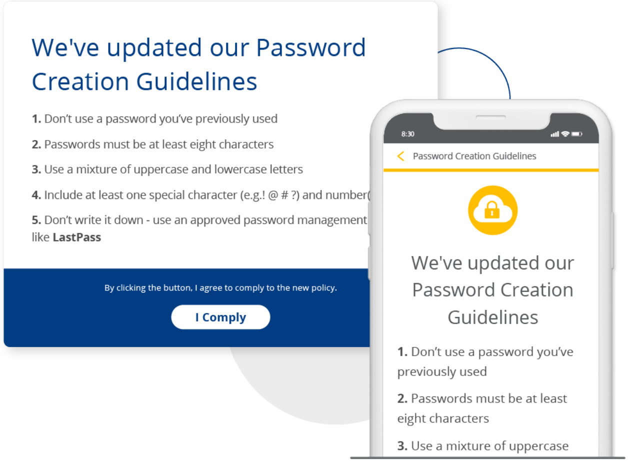


Important message from CEO

Our CEO Ashley Stewart would like you to watch this update

Leadership Comms

Important message from CEO



We've updated our Password Creation Guidelines

1. Don't use a password you've previously used

2. Passwords must be at least eight characters

3. Use a mixture of uppercase and lowercase letters

4. Include at least one special character (e.g.! @ # ?) and number(

5. Don't write it down - use an approved password management like **LastPass**

By clicking the button, I agree to comply to the new policy.

We've updated our Password Creation Guidelines

1. Don't use a password you've previously used

2. Passwords must be at least eight characters

3. Use a mixture of uppercase

Staff Compliance

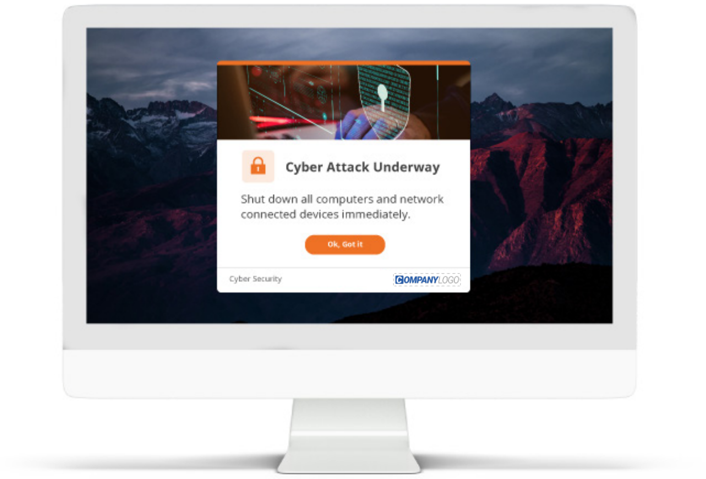
Virtual workforces increase your risk profile. In centralized workplaces, staff benefit from exposure to regular messaging and act appropriately due to a feeling of greater scrutiny. Employees working remotely are more likely to click on phishing emails because they're not 'in the loop' or may be distracted by activities unrelated to work.[6]

Action: Include a mandatory 'I accept' button in all policy update messages to staff, which all employees must click to acknowledge that they understand the policy and agree to comply with it. Send the messages to employees repeatedly until they acknowledge the policy and terms.

Security Breaches

Staff must be notified immediately in the event of a security breach or cyber-attack. Every second is critical in resolving the situation and minimizing the fallout. Clear systems must be in place to reach everyone in the organization, whether desk-based staff, remote workers or contractors.

Action: Have pre-built cyber security alert templates (with pre-agreed approval steps in place), ready to go when an event strikes so you can message staff with the click of a button. Time spent creating messages and seeking approvals in the heat of the moment is time lost on further damage and on resolving the incident.



Cyber Attack Underway

Shut down all computers and network connected devices immediately.

Cutting Through the Comms Clutter

Workplaces are noisy. Employees are busy and distracted. Most messages sent to them won't be read. That's a big risk for Information Security Managers. Every missed message can cause a costly mistake.

> **"Information security is the responsibility of every single person in the organization. If they have any access to data, they need to consider information security as part of their role."**
>
> – Angela Henry, Information Security Operations Head, South African bank

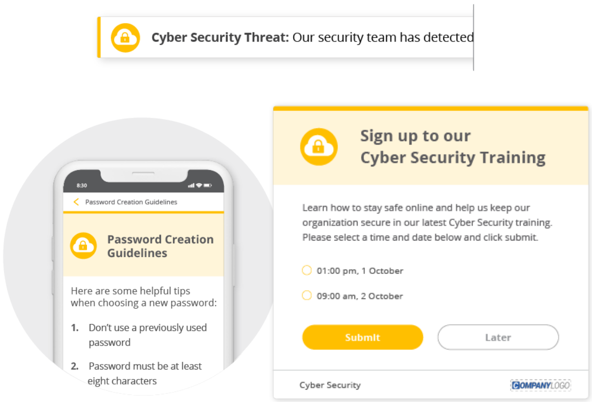
Successful communication means delivering InfoSec messages in a way that gets employee attention. Understanding how people process information is the key to achieving this. Appropriate, consistent, well-designed communications overcome selective attention, improve engagement and strengthen long-term recall.

Construct your messages using these tactics to get seen and be remembered.

Consistent Representation

Delivering content in a consistent style and manner helps employees create a mental 'short cut'. Recognition happens instantly and readership is increased.

Action: Use a dedicated color theme for all InfoSec communications. Display pop-up messages to staff in the same place on desktop screens.



Cyber Security Threat: Our security team has detected

Password Creation Guidelines

Password Creation Guidelines

Here are some helpful tips when choosing a new password:

1. Don't use a previously used password
2. Password must be at least eight characters

Sign up to our Cyber Security Training

Learn how to stay safe online and help us keep our organization secure in our latest Cyber Security training. Please select a time and date below and click submit.

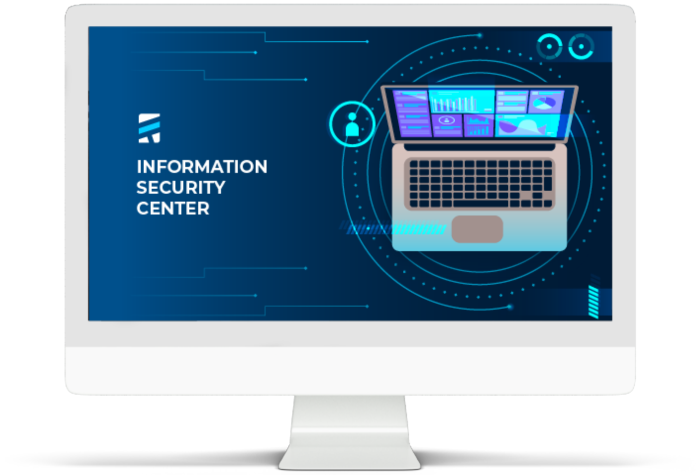
○ 01:00 pm, 1 October

○ 09:00 am, 2 October

Visual Cues

Including visual cues in your messages increase cognition and information processing. Employees are better able to recognize and recall the content associated with the visual.

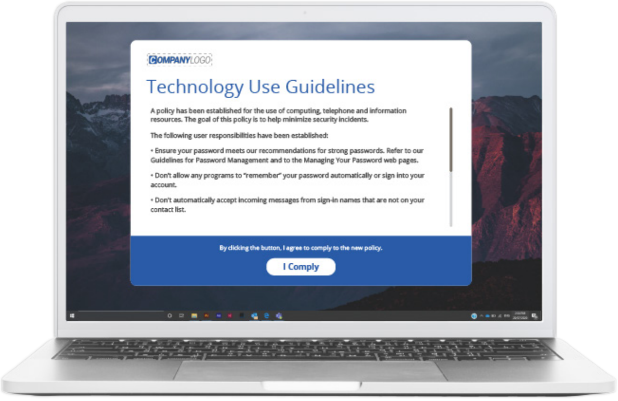
Action: Create an Information Security brand which gives the subject and all your messages a unique identity. Use this on all your communications.



Repeat, Repeat, Repeat

Reinforcement is essential to redress natural memory erosion over time. Repeated exposure to messages encourages memory retrieval, which contributes to learning.

Action: Use complementary channels to build understanding. Target repeat messages to specific employee groups, such as those that fail phishing simulation exercises.



COMPANYLOGO

Technology Use Guidelines

A policy has been established for the use of computing, telephone and information resources. The goal of this policy is to help minimize security incidents.

The following user responsibilities have been established:

• Ensure your password meets our recommendations for strong passwords. Refer to our Guidelines for Password Management and to the Managing Your Password web pages.

• Don't allow any programs to "remember" your password automatically or sign into your account.

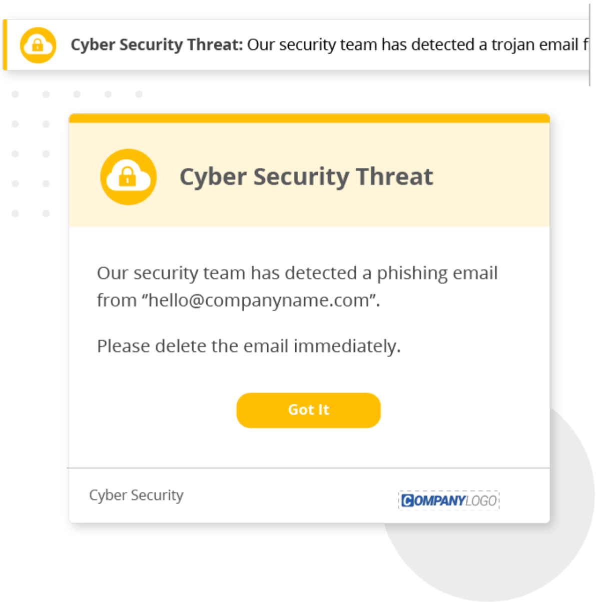
• Don't automatically accept incoming messages from sign-in names that are not on your contact list.

By clicking the button, I agree to comply to the new policy.

Message-Channel Fit

Messages should be sent in the channel best suited to the content. Emails are unsuited to urgent communications – their volume is high and readership low. Intrusive formats should be reserved for priority messages only.

Action: Select channels aligned to your communication objective. Immediate readership: pop-up alerts. Updates or reminders: emails or scrolling tickers. Employee feedback: online surveys.



Cyber Security Threat: Our security team has detected a trojan email f

Cyber Security Threat

Our security team has detected a phishing email from "hello@companyname.com".

Please delete the email immediately.

> **"We know people don't read emails... You don't know how many people are actually paying attention or clicking through."**
>
> – Service Operations Manager, Major UK healthcare provider

Building an InfoSec Campaign

Bringing all these elements together into a successful communication campaign creates the resilient human firewall that helps protect your organization.

Single messages delivered through a single channel are rarely effective for reaching employees. Higher message frequency builds employee awareness. Broader channel mix improves understanding and ultimately drives outcomes.

Communication Campaigns = **Higher Frequency x Broader Channel Mix**

Adopting a campaign approach to your internal communications:

- Guarantees delivery, readership and measurability
- Ensures compliance with important messages
- Drives behavior change
- Provides measurable outcomes

This compressed timeline illustrates how campaign performance is increased through delivering well-constructed messages via complementary channels. The cumulative effect is to make InfoSec communications more effective – becoming a powerful agent for positive behavioral change.

9am	Staff login and see wallpaper promoting your new initiative	Creates interest
10am	Their attention is grabbed by a pop-up alert	Grabs attention
Midday	They're updated by scrolling ticker and directed to your intranet for more detail	Informs & builds
4pm	Their understanding is tested in a light-hearted quiz	Maintains interest
Throughout the day	Staff are reminded of the initiative through prominent digital signage	Reinforces message
Throughout the week	Leadership sponsorship via video, phishing simulation via email, FAQ and tips via newsletter etc.	Strengthens human firewall

Your InfoSec awareness campaign should consist of a series of messages. These will typically include a 'launch' message, multiple 'nurture' messages and a single 'validation' message.

Running campaigns in this way ensures that in the event of a cyber-attack or data breach, your urgent, high-importance messages are much more effective, because employees are already conditioned to respond correctly.

Today's cyber security threats demand a modern employee communications platform. When selecting a vendor, ensure they offer these key capabilities.

- Multi-device optimization – to reach staff across a variety of device types
- Multi-channel formats – to achieve diverse messaging requirements from critical to helpful
- Accurate real-time reporting – to measure communications effectiveness
- Stringent security protocols – compliance with the highest standards of data security

Launch messages aim to create awareness of a new policy, resource on your intranet, update on company security performance or the beginning of Cybersecurity Month.

Best channels to use: Desktop alert, intranet

Nurture messages deliver information in a sequence to build employee knowledge and support positive behavioral change.

Best channels to use: Digital signage, screensaver, desktop ticker, email, newsletter

Validation messages are used at the end of a campaign to require employees to acknowledge or validate their understanding.

Best channels to use: Compliance alert, quiz

Sources

1. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

2. https://www.helpnetsecurity.com/2020/07/23/human-error-cybersecurity/

3. https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html

4. https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

5. https://www.helpnetsecurity.com/2020/05/20/ceos-cisos-disparities/

6. https://www.forbes.com/sites/hillennevins/2021/05/19/new-dangers-of-working-from-home-cybersecurity-risks/?sh=f60558922fb1

A New Approach to Cyber Security Communications

A robust human firewall is essential for cyber security in today's workplaces. But traditional methods of communicating with employees are no longer effective.

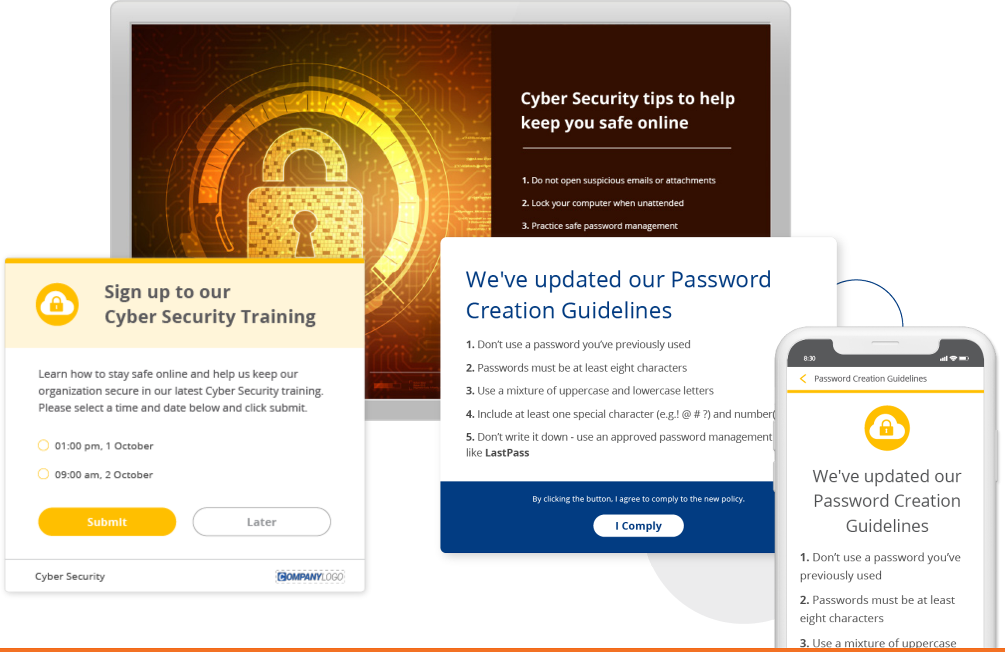
SnapComms is the global leader in multi-channel business-to-employee communications. Our award-winning digital channels are used daily by millions of users in 75 countries.

Our platform bypasses email and displays direct-to-screen – no email-overload, no chat distraction. Powerful, highly visual channels include Desktop Alerts, Tickers, Lock Screens, Quizzes, Surveys and Newsletters across desktop, mobile and digital signage.

We help leading organizations across the world with their InfoSec and broader IT communications.

SnapComms is an Everbridge Company, providing the only end to end critical event management and employee communication solution in the world.

Find out more by contacting us or taking a free trial.



Cyber Security tips to help keep you safe online

1. Do not open suspicious emails or attachments
2. Lock your computer when unattended
3. Practice safe password management

Sign up to our Cyber Security Training

Learn how to stay safe online and help us keep our organization secure in our latest Cyber Security training. Please select a time and date below and click submit.

○ 01:00 pm, 1 October

○ 09:00 am, 2 October

We've updated our Password Creation Guidelines

1. Don't use a password you've previously used
2. Passwords must be at least eight characters
3. Use a mixture of uppercase and lowercase letters
4. Include at least one special character (e.g.! @ # ?) and number(
5. Don't write it down - use an approved password management like **LastPass**

By clicking the button, I agree to comply to the new policy.

We've updated our Password Creation Guidelines

1. Don't use a password you've previously used
2. Passwords must be at least eight characters
3. Use a mixture of uppercase