



# Inspired eLearning April Newsletter



## SECURITY AWARENESS TRAINING FOR THE REMOTE WORKFORCE

Organizations across the globe are requiring their teams to work remotely to help protect against growing health concerns related to the COVID-19 virus.

[LEARN MORE](#)



## SECURITY AWARENESS TIPS SCREENSAVERS

Our new security awareness screensavers are a great way to share cybersecurity best practices with your organization every day.

[DOWNLOAD NOW](#)

### A message to our customers regarding COVID-19

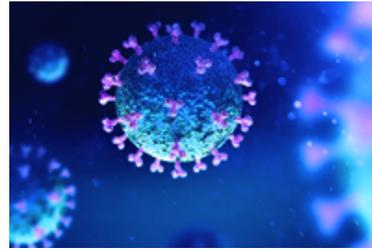
As efforts around the world to contain the expansion and impact of COVID-19 continue, we wanted to let you know what's going on at Inspired eLearning.

First, we remain dedicated to the health and wellbeing of our employees and community. In early March our employees began working from home for the foreseeable future. This transition was a simple one for our team, as fortunately, we all have the capacity to work from home. Second, we remain dedicated to providing you with the same level of exceptional service and support. We are here for you, so please reach out when you need us.

Due to the nature of our business and our agile workforce, you can be confident that it's business as usual at Inspired eLearning. This includes:

- Maintaining our hours of operation, which are 8 am – 5 pm CST

- Providing technical and account support via phone, email and video conference during business hours
- Keeping our retail website, iLMS, PhishProof, systems and all other programs and services running without interruption 24/7



Together, let's stay vigilant against cyberthreats (more info [here](#)) and follow appropriate guidelines from our public health agencies as we navigate through these challenging times. We will continue to monitor this rapidly evolving situation and will provide further updates to our business continuity plan and global operations as necessary.

---

### **Criminals Selling Videoconferencing Credentials on Dark Web**

As the number of cases of Zoom bombing has risen and companies lock down their videoconferencing calls behind passwords, attackers are now posting and selling videoconferencing credentials online, two security firms said this week.



In one case, a cybercriminal posted a database on the Dark Web containing more than 2,300 usernames and passwords for Zoom accounts, where the credentials could be used for denial-of-service attacks and pranks such as Zoom bombing, as well as potentially for eavesdropping and social engineering, says Stay Maor, chief security officer for global threat intelligence firm at IntSights.

"If the attacker can identify the person whose account he has taken over — and that doesn't take too much time, just use Google and LinkedIn — then the attacker can potentially impersonate that person and set up meetings with other company employees," Maor says.

"This can be used for business email compromise [BEC] types of attacks, where the attacker can impersonate a person in the company and ask to move money. It can also lead to asking people to share files and credentials over the Zoom chat."

In a second incident, a cybercriminal posted more than 350 Zoom account credentials to an online forum, with several belonging to educational institutions, small businesses, and at least one healthcare firm. The intent of the publication was to allow pranksters and vandals to disrupt video calls.

As the world moves to remote work en masse, attackers and security researchers have started testing the applications and services that now form the foundational infrastructure of everyday business. In addition to phishing attacks incorporating coronavirus- and pandemic-related topics as a lure to get employees to click on links, attackers have increasingly targeted virtual private networks (VPNs) and remote desktop protocol (RDP) services to attempt to exploit remote workers insecure home environments.

Videoconferencing applications are just the latest tool to attract attacker attention.

This article was originally posted by Dark Reading. Read the full article [here](#).

---

## Cybersecurity Lawyer Who Flagged The WHO Hack Warns Of 'Massive' Remote Work Risks

Large numbers of companies are rolling out mandatory work-from-home policies to help limit the risks posed by the coronavirus outbreak. But cybersecurity experts warn that those remote setups invite new hacking risks.

The Federal Bureau of Investigation recently issued warnings of an uptick in fraudulent crimes tied to the coronavirus, particularly by scammers posing as official health agencies.

This month, a hacking group tried to break into the World Health Organization. The breach was discovered by Alexander Urbelis, a hacker-turned-information-security lawyer who founded the New York-based Blackstone Law Group.



Although Urbelis can't be certain about the identity of the hackers, he says the group replicated a portal used by remote WHO employees that he describes as "very, very convincing."

Urbelis spoke with NPR's Steve Inskeep about the designs of such attacks and some best cybersecurity practices people should use to defend themselves against hackers.

### On how he spotted the cyberattack targeting WHO

The group that targeted the WHO, we have been watching for quite a while. And that group has in fact targeted several of our other clients [Editor's note: WHO is not one of Blackstone's clients.] And we have been monitoring the Internet for indications that the group has reawakened or reactivated some of its infrastructure. And that's what we detected with respect to a live attack against the World Health Organization.

### On the "sophisticated" group that targeted WHO

It's very difficult to say with any near certainty exactly who this is.

What we do know, though, is that the group that we've been watching is very sophisticated. Their attacks are very sleek. They're very well researched. The attackers perform a significant amount of reconnaissance on the configurations and the systems of [who they attack]. And they painstakingly create portals that look exactly like the victims' portals.

And that's what we saw with the WHO on the 13th of March. We saw a URL – a Web address – being created and put together that exactly mirrored the doorway to World Health Organization's internal file systems. So it was the external link to the internal file systems – that portal that

remote employees would use to access the WHO, let's say if they were working from home – that's what this group had replicated.

### **On how the "very, very convincing" WHO attack demonstrates the security issues with working from home**

People are very used to seeing these portals that are asking for their usernames and passwords. And if you look at the Web address or the URL that's associated with this particular type of attack, it was very, very convincing.

I was glad to hear, on the back end of this though, from what we know from the WHO, that the attack was unsuccessful.

### **On "the massive amount of security issues surrounding working from home."**

This means that more personal devices, more off-premises endpoints, so to speak, being used to handle and process business data, including highly sensitive data like trade secrets and business plans.

Because of this, all of our [client] companies have had to dedicate a massive amount of IT resources to support all of these remote working arrangements, including the deployment of best cyber hygiene practices – things that are known as MFA [multifactor authentication] or 2FA [two-factor authentication], in particular ... using something other than just a password to access company resources is critical these days. Because the bad guys know that people reuse passwords or they have variations on a theme of passwords.

There have been so many data breaches with all of our passwords for so many years now that there's always a password that you can associate with an individual. And so what the bad guys, the threat actors, will try is password spraying – just taking your username with your password and variations on a theme of your password and trying to brute force their way into your office systems.

This article was originally posted [here](#).

---

## **Product Updates**

We have exciting new updates to share! Click below to learn more about what Inspired eLearning is doing to better our product experience for our customers.

LEARN MORE

---

Connect with us:



© 2020 Inspired eLearning, LLC. All rights reserved.

info@inspiredelearning.com | 800.631.2078

4630 N Loop 1604 W, Suite 401

San Antonio, TX 78249 USA

[Privacy Notice](#)