jumpGuide

ivp

Protecting Your Employees Online

by Zack Willis on behalf of IVP

Helping your employees shield themselves from an ever-expanding list of online threats is crucial for any organization. This jumpGuide includes a series of safety recommendations that IT professionals should consider sharing with their workforces. This is a companion guide to the **Protecting Your Company Online** jumpGuide.

How an IT professional (me) almost got scammed online

One recent morning, I woke up to 500+ new emails. The messages were all spam but had made their way to my Gmail inbox — mostly confirmations of newsletter subscriptions I hadn't signed up for, strange emails in Russian or nonsensical junk.

By noon I had over 1K of these emails. I then started getting junk text messages — including one from Apple confirming an iPhone order and letting me know it would soon be ready for pickup at the Stanford Apple Store.

I assumed this was also spam. But I then logged into my credit-card account, just to make sure, and saw a charge from Apple for more than $1,000. I canceled my card and called Apple to cancel the fraudulent order.

By 3 p.m. I had more than 6,000 junk emails.

These events were clearly related. Soon, I realized that the reason for the avalanche of spam emails and texts was to obscure the legitimate emails from Apple confirming my order, as well as whatever else this bad actor was trying to buy with my credit card. Smart, as there was no way I would have seen the Apple emails. Thankfully, Apple took the extra step of texting me.

The interesting and scary thing is that the scammer was evidently a local person who planned to go to Stanford to pick up this iPhone, which means he must also have had a fake ID with my name on it. (Apple won't release an order without the buyer's identification). I ended up with 7.5K spam emails, which abruptly stopped around 4 p.m. — likely when the scammer or scammers realized the ploy hadn't worked. I got one more around 5 p.m. saying a loan application in my name had been denied. Thankfully, my credit is frozen.

The Takeaway: Remember that your Social Security number, old and current passwords, credit card numbers and more ARE on the dark web. Protect yourself by freezing your credit, using strong random passwords and enabling 2 Factor Authentication (2FA) on everything.

What employees should do to protect themselves

Take advantage of tools and services:

- Optery to remove your data from the internet
- SpyCloud to get alerts when your passwords are found on the dark web
- The Duo mobile app to enable 2FA on all your personal accounts
- Create a free 1Password account and link it to your work account (if applicable), and use it to generate all of your personal passwords

Turn on 2FA on all your accounts

How to: https://2fa.directory/

Freeze (don't lock) your credit at all 5 (yes, 5) bureaus

Links to all the bureaus plus why this matters

Decide whether to register yourself for USPS Informed Delivery before a hacker does

- USPS link
- Why taking this step requires understanding the pros and potential cons

Permanently opt out of credit card and insurance offers

- Opt-out link
- Read why this matter

Register yourself on the Social Security site before a hacker does

- SSA link
- Read why this matters

Register yourself on the IRS site before a hacker does

- IRS link
- Read why this matters

Register your Franchise Tax Board account before a hacker does

- https://www.ftb.ca.gov/myftb/create-an-account.html

Call your cell provider and add an authentication password or PIN and turn on extra sign-in security (2FA).

- AT&T: 800.331.0500 – More info
- Verizon: 800.922.0204
- Read why this matters

Use an ad/cookie blocker on all your computers and mobile devices

- Not only does this prevent sites from tracking you across the internet, it also helps protect you from malware/viruses
- I recommend uBlock Origin for your computers and Purify for your mobile devices

Blur out your house on Google Street View and related apps

- Street View makes it easy for bad actors to virtually case your house and cars, to study how to gain illegal access. Here's more info
- How to blur on Apple, Bing and Google

Learn how to spot phishing emails and text messages

Phishing Behaviors

- Creates false urgency, e.g., “I need you to do this immediately…”
- Includes content that is vague or looks/feels slightly off
- Asks you to click on a link and/or open an attachment
- Asks you for personal information like your password, bank account information or personally identifiable information
- Is unsolicited and unexpected – do you receive such emails or texts at this address?
- Feels impersonal – “From HR” or “From (Company)” vs. someone you know

In-message Phishing Clues

- Misspelling of common words
- Misspelling of domain/company name in sender address
- The message is from a different domain than the official one (e.g., google.com is real but google-account.com or google.us is not)
- Hovering over the link shows a different address than the content specifies

General Tips

- Slow down – when you stop and analyze before acting, security wins
- Always question the message and start with a healthy suspicion
- Unsure? Reach out to your IT department or directly to the person in a different form of communication, such as a phone call

Turn off auto download for images in your email

- By default, email images are automatically downloaded. The problem is, you don't know what exactly you are downloading. It could be a tracker to see if you've read the email, it could be malware or it could be an innocuous gif. I recently turned off auto download in Outlook Mobile and I've had newsletters emailing me asking why I am no longer reading their emails (they can no longer track me, which is great).
- How to do this on most email clients

Remove your personal information from online brokers

- Your personal information is all over the internet. Your phone number, address, full name, birthday, kids' names and so on. This information gives hackers everything they need to send you a very realistic phishing email, call or text you pretending to be a legit service or scam you in other ways, including stealing your identity. This is also how credit-card companies, newsletters and the like get your information and spam you.
- Optery is a service that will scrub your information from the internet. Check with your IT department. Your company might already be paying for that service.

Protecting your employees is not only the right thing to do; it's also good business. Providing your workforce the tools to avoid damaging and costly online scams, identity theft and security breaches helps the entire organization stay focused on achieving its next level of success.

For questions about or feedback on these recommendations, please contact IT@ivp.com.
