# Don’t be haunted by the hacks

**Image:** Included in toolkit.

**Suggested Alt Text:** Scary-looking pumpkin, email with a “phishing” hook in it, open documents overlaying a laptop. The illustration represents that October is Cybersecurity Awareness Month and online threats are real.

October is the month of goblins and frights of all sorts. We expect ghost- and zombie-costumed trick-or-treaters and oversized plastic skeletons lining front yards across America.

What we don’t want to see this month — or any month — are the dreaded, dangerous online scammers. They want to get rich off you by accessing and using your credit cards, bank accounts, and hard-earned benefits. The consequences they cause, if successful, are real-life nightmares.

Slay scary scammers by staying aware, alert, and skeptical of anyone you don’t know contacting you via text, email, social media, or phone and asking for your personal information or for you to open links or attachments they send. Don’t do it. It’s not being rude. It’s protecting yourself and loved ones.

Top questions about staying safe online are “How do I stay safe?” “What should I focus on?” “How do I report scams or identity theft?”

Focus on four key behaviors to secure your world and keep safe online:

* **Recognize and report phishing.**

## At home, [Protect yourself against social media phishing](https://news.va.gov/105732/protect-yourself-against-social-media-phishing/).

## At work, report phishing using an email report spam feature if available or reporting it to your supervisor or security office.

* **Enable multi-factor authentication (MFA)**. Be sure you have MFA on all your accounts. For an overview, [check out the short multi-factor authentication video](https://youtu.be/PFQhtJSGmC0). If you need more help, call your institution (such as your bank or email provider customer service line) or ask a trusted and tech-savvy family member or friend how to do so.
* **Use strong passwords and a password manager**. Use a unique password that includes 12 to 15 letters, numbers, and symbols for each one of your social media accounts. Don’t repeat passwords and be sure to [change your passwords regularly](https://www.nist.gov/video/password-guidance-nist-0). You can also use a password manager, which will notify you if any stored login information is compromised.
* **Update software**. When it comes to [updating your software on mobile devices and laptops](https://digital.va.gov/cyber-spot/defending-digital-threats-one-update-at-a-time/), don’t ignore them.

**More tips here**

* [Bookmark and regularly visit the VA Cybersecurity Spot](https://digital.va.gov/cyber/) for updates on how to stay safe online.
* Report issues to your banks and financial institutions if you believe there is fraud or identity theft.
* Veterans who suspect they have been the victim of VA disability benefits fraud should call VA at 1-855-578-5492, right away.
* File complaints with the [Federal Trade Commission](https://reportfraud.ftc.gov/), [with the FBI](https://www.ic3.gov/Home/ComplaintChoic), and with the [Federal Communications Commission](https://consumercomplaints.fcc.gov/hc/en-us).

**Remember to Secure Your World.**